A/R 435

93-3
19-2

ADMIRALTY 195/45

ADM 1/27186

S (INT)

RETURN TO
R. O.

Review of Security of Naval Codes and Ciphers

Sept. 39 – May 45.

Issued by Signal Division Nov. 1945.

(1945)

TOP SECRET

Enclosure A. to
M.I.D 00517 53/46.

TOP SECRET

COPY No.1

REVIEW OF THE SECURITY OF NAVAL CODES AND CYPHERS -
SEPTEMBER 1939 to MAY 1945

NAVAL STAFF - SIGNAL DIVISION and NAVAL INTELLIGENCE DIVISION,
ADMIRALTY,
November, 1945.

ADMIRALTY 195/45.

TOP SECRET

Signal Division,
Admiralty.

10th November 1945.

Sir,

I have the honour to submit herewith a Review of the Security British Naval Codes and Cyphers, compiled by me and covering a period from the outbreak of hostilities on 3rd September 1939 until the end of the war with Germany in May 1945.

I have the honour to be,

Sir,

Your obedient servant,

Commander(S), R.N.

To: The Director of Naval Intelligence
(Copy to Director of Signal Division).
Admiralty.

Distribution of copies: No.1, D.N.I.
No.2, D.S.D.
No.3, A.D.S.D.(S.C.)

TOP SECRET

SECURITY OF NAVAL CODES AND CYPHERS - REVIEW OF WAR EXPERIENCE.

TABLE OF CONTENTS.

Preface.

PART I.

Chronological record of Naval Cryptographic systems and procedures.

PAGE.

Section A - HIGH-GRADE SYSTEMS.

1. Book Systems, including Call Signs and Delivery Groups 1 - 29
2. Machine Systems ... ... 30 - 39
3. Special review of Naval Cypher as a British-U.S. high-grade system. 40 - 47

Section B - LOW-GRADE SYSTEMS. ... ... 48 - 53

Section C - MERCHANT SHIPS' SYSTEMS. ... ... 54 - 61

PART II.

PAGE.

Summary of Enemy cryptanalytical successes.

Preface 62

Section A - HIGH-GRADE SYSTEMS. ... ... -

1. Book Systems... ... ... 63 - 77½
2. Machine Systems ... ... 78 - 79

Section B - LOW-GRADE SYSTEMS ... ... 80 - 88

Section C - MERCHANT SHIPS' SYSTEMS ... ... 89 - 96

Section D - CALL SIGNS AND DELIVERY GROUPS ... ... 97 - 100

PART III.

General Conclusions, lessons learnt and recommendations for future policy.

Section A - HIGH-GRADE SYSTEMS, BOOK AND MACHINE ... ... 101 - 107

Section B - LOW-GRADE SYSTEMS ... ... 108 - 112

Section C - MERCHANT SHIPS' SYSTEMS ... ... 113 - 116

Section D - CALL SIGNS AND DELIVERY GROUPS ... ... 117 - 118

Section E - GENERAL. ... ... 119 - 121

Index ... ... 126 - 130

TOP SECRET

PREFACE.

This Review has been divided into three Parts. Part I is a departmental record of the systems and procedures used, and of action taken at different stages throughout the War to safeguard and improve the security of Naval cryptographic aids. It is self-contained as such and has been compiled independently of, and without reference to, the two succeeding Parts, which were prepared later in the light of information at our disposal respecting the nature and extent of German cryptanalytic successes. One object of Part I is to provide the responsible Divisions of the Naval Staff with a concise and chronological record which should be of assistance in conducting any future investigations into particular leakages of information to the enemy which might be suspected to have been due to exploitation of Signal Intelligence. Apart from this, however, the information incorporated in Part I is essential to a proper technical analysis of the many and varying factors which contributed to the insecurity of certain systems. In order to obtain a clear view of the security afforded by Naval cryptographic aids used during the war, it is not essential that Part I should be read in advance of, or in addition to, the succeeding Parts.

2. Part II embodies a record of German successes and failures in the solution of individual high-grade and low-grade systems. It has been compiled from a great mass of information now in our possession, resulting from interrogation of German Naval and Cryptographic personnel, and the examination of German signal logs and Signal Intelligence archives. As such, it is of very considerable general interest. In order to provide a true picture of enemy achievements in this sphere, the disclosures in Part II are related throughout to corresponding portions of the historical record in Part I, but in such a form that immediate references back to Part I are unnecessary.

3. Part III, which comprises general conclusions, lessons learnt and recommendations for future policy, is based largely on the disclosures in Part II, related again to Part I. Since the subject matter of this Part deals largely with future policy it is, from the practical aspect, the most important section of the Review.

4.....

4. The ultimate aim of this Review is to present an objective survey of the causes which contributed to the failure of certain of our cyphers and codes to withstand expert cryptanalytic attack,and, in the light of this knowledge, to formulate concrete proposals for the future. Beyond mentioning a few specific instances of outstanding interest, attempt has not been made to record in detail the strategic and tactical successes which must have accrued to the enemy by reason of his ability to break into a number of our cryptographic systems.

5. The length of this Review has been deliberately curtailed, since to have included in it an extensive digest of the voluminous documentary material available in Admiralty would have tended to cloud the main issues and so defeat the intention of giving a clear cut picture of our cryptographic successes and failures. All the material referred to has nevertheless been carefully sifted and evaluated, and it is believed that no salient features bearing on the subject matter of this Review have been overlooked.

6. Very little information regarding Japanese work on Naval cryptographic systems has been received in Admiralty up till the date this Review was concluded. However, the scanty evidence which has so far come to hand tends to confirm the expressed German opinion that the Japanese are relatively inept in the sphere of cryptanalysis,and to show that they achieved little if any success, certainly with our high-grade systems. The evidence is still, however, unconfirmed and pending receipt of information based on detailed interrogations and examination of Japanese Signal Intelligence documents, further speculation at this stage would be futile.

 TOP SECRET

PART I - SECTION A - HIGH GRADE SYSTEMS.

1. Book systems, including Call Signs and Delivery Groups.

At the outbreak of war in September 1939 there were three main high-grade Naval book systems, viz: Naval Cypher No.1 (S.P.02184) - a four-figure book in force since 1934; Administrative Code (S.P.02195) - a five-figure book, also in force since 1934; Auxiliary Code - No.3 - (S.P.02205) - a four-letter book in force since February 1937, for use by small vessels.

2. Naval Cypher was always used recyphered but the number of Tables was very limited, comprising five series only, namely the Commander in Chiefs' Table, S.P.02171, the Flag Officers' Table, S.P.02172, the General Table, S.P.02174 held by all ships except Destroyers and below, the Small Ships' Table, S.P.02175, and the China Gunboats' Table, S.P.02186.

3. The Administrative Code, which had been in force for some five years prior to the war, had been used very extensively throughout that period, unrecoded for non-confidential signals and, from 1938 onwards, recoded by means of one general series of Tables only (S.P.02211) for confidential signals. From February 1937 until April 1939, the Administrative Code had also been used as a Cypher with a special secret recyph-ering table (S.P.02210) held by the Cypher Staff. The security value of this Code at the outbreak of war was therefore very low.

4. The Auxiliary Code (No.3), which had been in force over 2½ years, had likewise during that period been used unrecoded for non-confidential traffic and recoded by a multiple alphabet table for confidential traffic. Its security was also therefore low. Both the Auxiliary Code and the Administrative Code were withdrawn from use on 20th August 1940 (see later).

5. In the years preceding the war, when of course the volume of secret and confidential traffic was low, the recoding and recyphering tables used with these three books changed at irregular and infrequent intervals. Some ten days before war broke out, however, steps were taken to change the more important tables; production of reserve editions of tables had

TOP SECRET

moreover been greatly accelerated early in 1939 in order to provide, if necessary, for faster changes of editions. Thus a new edition of the General Recyphering Table (S.P.02174(8)) was made effective on 25th August 1939 and on the same date new editions were made effective of the Commander-in-Chiefs', Flag Officers' and the General Administrative Code Tables. The recoding table for Auxiliary Code had been in force since 9th February 1937 concurrently with the basic book itself, and had necessarily to be reatained in force after the outbreak of war until 1st November 1939. Subsequent editions of this series became effective at approximately 3-monthly intervals until the system was abandoned on 20th August 1940.

6. The General (S.P.02174) and the Small Ships (S.P.02175) series of recyphering tables for Naval Cypher were retained as such until 20th August 1940. The Small Ships series then became the General series and the previous General Series (S.P.02174) was discontinued. The rate of change of editions of the General Series was greatly accelerated following outbreak of hostilities; thus, seven editions of that series were used between 25th August 1939 and 20th August 1940 - an average of one edition for about seven weeks. Similar acceleration in the rate of change of the Small Ships Tables took place.

7. The situation was less satisfactory with regard to the Auxiliary Code. As already stated this Code (No.3) had been effective since February 1937, and from then up till the outbreak of war had been used with one edition only of a multiple alphabet table. Owing to the shortage of follow-up editions, a new table could not be made effective until 1st November 1939, i.e. some three months after war broke out, and until this system was dispensed with in August 1940 it was found possible to introduce four more editions only. There were moreover no succeeding editions of Auxiliary Code itself available, so the latter (No.3) had necessarily to remain in force from the date of its original introduction (9th February 1937) until replaced by Naval Code on 20th August 1940.

8. Anglo-French codes- Since 1938 there had been in production in Admiralty two Anglo-French crypto.channels. The 5-figure Anglo-French Cypher and the 4-letter Anglo-French Code. The latter was made

TOP SECRET

effective early in 1940, using a simple substitution recoding table. After the collapse of France it remained in use for communication with Free French Naval forces, with of course different tables. Multiple Alphabet tables were introduced in 1943. Use of the Anglo-French Cypher was very restricted and confined almost exclusively to the West Africa Command; the Cypher was used with 15,000-group long-subtractor tables.

9. In May 1940, steps were taken to provide ships operating in dangerous waters with a special recoding (recyphering) table to be carried in place of normal tables and so minimise the risk of general compromise of Fleet communications. Initially, the table used was S.P.02319 (later to become the Area I Submarines table). It was used with Naval Cypher, and Delivery Groups were used if necessary to indicate when a message should be decoded by ratings. This arrangement was modified in June 1940, when a special edition (No.2) of the forthcoming S.P.02176 series (General table for Naval Code, not yet in force) was made effective as the surface-craft dangerous waters table, whilst S.P.02319, the previous dangerous waters table, was reserved for exclusive use by Submarines.

10. The first important wartime changes in our high grade book systems took place on 20th August 1940. On that date Naval Cypher No.1, which had been in force for some 6 years, was replaced by Naval Cypher No.2. Naval Code No.1. a new 4-figure book almost identical in design to Naval Cypher, was brought into force to replace the old Administrative Code. This was a great step forward since, externally, cypher traffic was now no longer readily distinguishable from code, and the task of the enemy analyst was correspondingly more difficult. One the same day (20th August 1940), new editions of the Commander in Chiefs' and Flag Officers tables were introduced. S.P.02175, which had hitherto been the Small Ships recyphering table, became the General table in place of S.P.02174. The new series of general tables for Naval Code (S.P.02176 series) was made effective on 20th August 1940, starting with S.P.02176A. A new series of long-subtractor tables for use with Naval Code, by Auxiliary Vessels, was also made effective on 20th August 1940. This was the S.P.02323 series, which replaced Auxiliary Code.

TOP SECRET

On 20th August 1940 use was discontinued of the old General recyphering table, S.P.02174 series, but certain editions were retained for use as Area Tables (see later).

11. The distribution of Naval Code was not, however, quite complete by 20th August 1940, and from that date until 2nd September 1940, Admiralty General Messages were made in Naval Cypher recyphered by the first edition of the new General Tables (S.P.02175 (12)).

12. In August 1940, the new Auxiliary Vessels Recoding Tables S.P.02323 series (see para.10) became the standard Dangerous Waters Tables for use by surface-craft, thus replacing the special edition of S.P.02176 hitherto used for this purpose (see para.9).

13. From 20th August 1940, use of the Auxiliary Code and its multiple alphabet table was discontinued generally, but Auxiliary Code was retained temporarily for local use, unrecoded, by auxiliary craft when speed was vital.

14. Area Tables - Early in 1940, it became apparent that in order (a) to reduce the load of traffic on certain of the long-subtractor tables which was showing signs of increasing beyond the safety limit, and (b) to safeguard world-wide Fleet communications from possible compromise by reason of the loss of a table in a particular area or during a special operation, some system of recoding and recyphering tables must be instituted by which the effects of loss, or compromise by other means, of an individual table should be isolated so far as practicable to the area in which the compromise took place. A system was therefore introduced by which the existing General tables would remain effective for world-wide use, but a number of new series were produced and distributed for use exclusively within certain Areas.

15. For this purpose, three distinct Areas were established, viz:

Area 1 - Home Station and Atlantic North of Equator

Area 2 - Mediterranean, East Indies and Atlantic South of Equator

Area 3 - China, Australia and New Zealand Stations.

TOP SECRET

16. Production of all the necessary Area Tables was already in hand, but pending such time as they could be distributed and made effective, six unused editions of the old S.P.02174 series (general re-cyphering tables which had become obsolete on the 20th August, 1940, concurrently with the introduction of the new basic books) were set aside for use as Area I and II re-cyphering tables. Number 15 was effective on the 5th October, 1940, for Area I, and number 16 on the same date for Area II. From this date onwards, Area I and II re-cyphering tables were continually effective. From the 21st November, 1940, ~~and~~ onwards, the new Area Tables started to become effective: thus on the 21st November, 1940, the Area I re-coding table S.P.02355(1) became effective: on the 29th November, 1940, the Area I Auxilliary Vessels Table S.P.2358(1) and Area I Dangerous Waters Table S.P.02361(1) were effective; on the 1st January, 1941, the Area II Submarine and Auxiliary Vessels Tables became effective, etc.

17. Further Dangerous Waters Tables. Meanwhile, in addition to the extra tables referred to, production had been put in hand of further series of Dangerous Waters Tables for use with Naval Code. On the 17th January, 1941, the world-wide Dangerous Waters Table, S.P.02350, and the Area II Dangerous Waters Table, S.P.02362, became effective; these were followed on the 1st March, 1941, by the Area III Dangerous Waters Table, S.P.02363. By early in 1941, we had therefore in force an extensive system of area tables including area Dangerous Waters Tables.

18. Recoding Procedure. It was decided in 1940 to introduce as a security measure the "Left and Right " procedure for re-coding messages by means of long-subtractor tables. This involved the re-coding of the address portion of the message on the left-hand pages only of the table and the subject matter on the right-hand pages, starting from the corresponding right page group following the left page group at which re-coding of the address ceased. This had the advantage of providing, in effect, an entirely separate table of 7,500 groups for recoding the more stereotyped address groups taken from the basic book, i.e. those groups more susceptible to cryptographic attack.

TOP SECRET

It had, of course, the corresponding disadvantage of halving the number of groups available in each table for recoding the great bulk of groups comprising the subject matter of each message. This procedure was made effective on the 1st October, 1940, for all tables except the Auxiliary Vessels Re-coding Tables for Naval Code. It was thought undesirable to impose this additional complication on the coding personnel of small ships. It was later, however, made effective for the Auxiliary Tables. (on the 1st October, 1941). This procedure continued to be effective throughout the War for all long-subtractor tables used with Naval Cypher and Code, except that it was not used with the British-U.S. Naval Cypher (III) until the 1st August, 1942.(see special review of British-U.S. Cypher).

19. Indicator Procedure. For a number of years before the War and during the War up till 19th January, 1941, the indicator system was for a five-figure table indicator to be chosen from a book of indicators (S.P.02169) which remained unchanged for a very lengthy period. This indicator showed against it a letter denoting the series of table used, and was inserted as the first and last group of the message. The starting point indicator was a five-figure group chosen from a list of such groups at the beginning of the appropriate table and against which was shown the page and line of the table at which re-coding started.

20. Early in 1941 it became evident that with the steadily increasing volume of traffic a modification to this procedure was desirable. On the 20th January, 1941, therefore, the following disguise indicator procedure was made effective for all long subtractor tables except the Submarines and Auxiliary Vessels series:-

(a) Starting point indicator chosen from front of table in normal manner and the message re-coded starting at the page and line indicated, the first re-coded group being inserted in the third space on the message form.

(b) Table indicator chosen from S.P.02169 and inserted as the first and last groups of the re-coded message.

(c) The starting point indicator chosen at (a) was then disguised by adding to it three dummy digits chosen at random, thus making eight digits, and these eight digits were subtracted from two consecutive number groups on the last page of the re-coding table, the first of which was indicated by the initial two digits of the table indicator.

TOP SECRET

(d) The resulting eight digits were inserted as the second and third groups of the re-coded message and repeated in the same order at the end of the message immediately preceding the (check) Table Indicator.

21. This system eliminated to a large extent the danger of "presented depths". It did not overcome the danger by which an indication of the series of tables used was disclosed by reason of using Table Indicators from a book which had remained in force for a long time; on the other hand, however, it introduced the very real security advantage of concealing the true starting point Indicator from the enemy, and so hindering his endeavours to segregate, for special analysis and attack, numbers of messages which he could assume, from recovery of Table Indicators and from the appearance of identical Starting Point Indicators, (coupled with W/T I), to have been recoded by the same table and from the same starting point. This system remained in force until the 1st September, 1941 (see later).

22. On the 17th March, 1941, a "Ship Index" (S.P.02329) was made effective for the coding and cyphering of names of warships not included in the basic books. Part II of this Index (Signal Letters of Merchant Ships) was not used. This book remained in force throughout the War. Its use was later very much restricted owing to introduction of Lists of Navy Numbers (see later).

23. In April 1941, a disguised indicator system, similar to the one referred to above, was introduced for use with R.A.F. Station Cypher, which at that time was the standard high-grade inter-service book system.

24. On the 16th April, 1941, the "Single Letter Spelling Table" provided in Naval Code and Cypher was cancelled since it had become apparent that this system (by which A was coded as 01, B as 02, etc.) was prejudicial to security. From this date onward, spelling was done by the syllabic method, or by use of the four-figure groups provided in the basic books for each letter of the alphabet, or by a combination of both methods. Editions of Naval Cypher and Naval Code, produced from this date onwards, were provided with bigram spelling tables.

25. By the early part of 1941 it became evident that with the enormously increased volume of traffic in high-grade book cyphers, many conceptions previously held about the security of the long-subtractor

system no longer held good, and that numerous references and instructions on the matter which appeared in S.P.02217 (the "Manual of Cyphering and Security" then in force) required modification. In May 1941 the Fleet was warned by General message that certain rules from which Grade 1 systems had hitherto been excepted, on account of their (supposedly) very high security, must in future be adopted. It was pointed out that the statement in S.P.02217 that "Grade I codes and cyphers are considered to be unbreakable provide the few simple rules for their use are faithfully complied with" was no longer entirely true; also that the loss of a basic book was equally serious to the loss of a Table. Grade I systems were no longer excepted from the rules (hitherto applicable only to Grade II systems) regarding re-encypherments, publication of plain language versions, transmission in plain language of references to the subject matter of coded messages and to their times of origin, etc.

26. In June 1941, there occurred a number of losses of unused tables which interrupted the programme of changes and necessitated certain tables remaining in force for longer than the normal periods. From June 1941, however, all our recoding and re-cyphering tables were changing twice monthly except:-

C-in-C's Table, approximately every two months.
Flag Officers and Auxiliary Vessels Tables, monthly.
Dangerous Waters General Table, at irregular intervals varying between one and three months.
Area Dangerous Waters Tables, one month in Areas II and III; approximately two months in Area I.

27. On the 16th June, 1941, Naval Cypher No. 3 together with the "H" and "M" re-cyphering tables was made effective as the British-U.S. Naval Cypher (see separate review). The setting aside of this edition necessitated retention of (intra R.N.) edition of our own Naval Cypher (No. 2) in force much longer than was originally anticipated. It had become effective as far back as 20th August, 1940, and had necessarily to remain in force until 1st January 1942.

28. One Time Pads first made their appearance in June 1941. Their use was limited initially to Two-Way Navy Pads S.P.02341, to Admiralty OUT pads (S.P.02403) for a special category of messages to certain Flag Officers, and S.P.02407 for other secret messages to Flag Officers who held the Flag Officers table S.P.02172.

TOP SECRET

The S.P.02403 series started to be used on the 16th June, 1941, and the S.P.02407 series on the 18th July, 1941. The introduction of these pads, which of course provided one hundred per cent security, was something of a milestone in communications security. The advantages attached to their very extensive use for naval communications was appreciated, and many more series were at once put into production with a view to providing the Admiralty and all Commanders-in-Chief with an entirely secure means of "Out" communication to Major War Vessels and authorities. Production was also put in hand of "Navy Three", "Navy Six" and "Navy Twenty" pads for intercommunication between limited numbers of authorities. No attempt was made at this stage to disguise One Time Pad Indicators; the starting point and, in the case of two-way pads, the pad number, was denoted by self-evident groups. Use of the S.P.02403 and S.P.02407 series were likewise indicated in clear.

29. Naval Shore Code. A secure high-grade Code for communication with Reporting Officers over Naval and shipping matters, and with Consular Shipping Advisers, Naval Control Service Officers and Naval Attachés, etc., had become a requirement in 1940 to replace the Government Telegraph code (recoded) and the Interdepartmental Cypher, which had hitherto been used for this purpose. The G.T.C. recoded was unsatisfactory both from the security aspect (since the Naval tables used with it were simple bigram-substitution ones affording very low security) and from the practical coding aspect since G.T.C. is not of course well adapted for Naval phraseology. The Interdepartmental Cypher was likewise unsuitable both on account of its vocabulary and because the general series of long-subtractor recyphering tables used with it received a very wide distribution throughout all the Services and Foreign, Dominions and Colonial offices. Their security either from physical compromise, or compromise by excessive use or mishandling, could never therefore be guaranteed.

30. A new basic book, "Naval Shore Code" had therefore been prepared to meet this requirement, and was made effective on 12th July, 1941. This book was designed on the lines of Naval Cypher and Naval Code, but with a vocabulary specially adapted to its requirements.

TOP SECRET

Concurrently with its introduction, three series of Area Recoding Tables of the normal long-subtractor type were made effective. These tables were changed automatically every three months until the 1st January, 1943, when a monthly change of edition was introduced. A general (world-wide) table was made effective, with monthly changes, from the 1st December, 1942. The code was used plaindress and the "Left and Right" recoding procedure was not effective. The address was expressed in G.T.C. In order to limit, sofar as practicable, the volume of traffic in this code which should be available to the enemy for analysis, messages in it were ordered to be routed by cable whenever practicable. Throughout the War, extensive use of one time pads of the two-way series was made with this code, particularly for communications between Admiralty and Naval Attaches and between Naval Attaches and posts in their areas particularly vulnerable to sudden enemy attack.

31. As stated earlier, production was now in hand of further series of One time pads for use by Admiralty and Commanders-in-Chief as "Out" pads to all ships and Authorities in certain areas. An important and early requirement was a means of One Time Pad communication from Admiralty to holders of Naval Cypher in Area I (Home and North Atlantic), and one of the new series (S.P.02416) was in hand to meet this requirement. Pending its introduction however, a special edition of the general recoding table for Naval Code (S.P.02176(25)) was set aside for use by Admiralty as an Area I "Out" One Time Pad. It was made effective 20th July, 1941. Self-evident indicators were used to denote the table and the starting point, e.g., "217625 0101." This table was followed by successive editions of the Area I recyphering table (S.P.02352), especially allocated for the purpose, until the new One time Pads (S.P.02416 series) were eventually made effective on the 15th December, 1941.

32. In August 1941, analysis showed that the Area I Auxiliary Vessels Recoding Table (S.P.02358) was carrying an alarmingly heavy load of traffic. Editions were changing monthly at this time, and reserves did not allow of acceleration. A general warning was issued to the Home Station to restrict traffic in this table to an absolute minimum and, in drafting messages, to avoid stereotyped phraseology.

TOP SECRET

The Auxiliary Vessels Recoding Tables were throughout the War particularly susceptible to cryptographic attack by reason of the Auxiliary Vessels Call Signs used with them.

33. On the 1st September, 1941, the system of disguised Starting-Point Indicators referred to earlier was discontinued in favour of a new system using undisguised 4-figure Starting-point Indicators concurrently with a new edition of Table Indicators and introduction of rapid changes of editions of the latter. The advantages claimed for the new system were firstly that, by reason of the rapid changes of the Indicator Book it would be far more difficult than hitherto for the enemy to classify table indicators into their respective families; secondly, the intention was that there should be one, and one only, family of four-figure Starting-point Indicators common to and appearing in all Tables (although of course with different page-line significations in each different edition of every series). The fact that two or more messages intercepted by the enemy bore identical starting point indicators would (in theory) no longer therefore be an indication that each message had probably been re-coded by the same table and starting at the same point. In order to hasten introduction of this new system, appendices had been prepared and distributed for use with existing tables; these comprised lists of four-figure Starting-point Indicators for use instead of the five-figure ones printed in the tables. All future editions of tables were, of course, produced with four-figure Starting-point Indicators.

34. Concurrently with introduction of this new procedure, a new edition of the Table Indicator Book (S.P.02169(2)) was made effective to replace the heavily used first edition which had been in force for a number of years. The rate of production of editions of the Table Indicator Book was greatly accelerated, and subsequent editions were made effective at approximately two-monthly intervals until the 1st June, 1942, from which date, until the end of the War, editions were changed monthly. For reasons given later, the new procedure did not fulfil expectations and it was discontinued on the 15th December, 1942, when a return was made to disguised Starting-point Indicators.

TOP SECRET

35. In September, 1941, it was decided to set aside a special table for use by Commander-in-Chief Western Approaches for recoding his daily situation reports. These reports had hitherto been recoded in the normal edition of the Area I Auxiliary Vessels Table (S.P.02358 series) and the length of the signals, coupled with their very stereotyped subject matter, was a source of danger to the security of that Series. From the 18th September, 1941, therefore, until the introduction of the Commander-in-Chief Western Approaches Code "Out" pads on the 21st January, 1942, the Admiralty set aside special editions of the Area I Auxiliary Vessels Table for use exclusively by the Commander-in-Chief Western Approaches for his situation reports. Use of these special editions was denoted by a self-evident indicator showing the series (2358) followed by two digits showing the edition number, e.g., "235811". The table was not used as a One-time Pad. Normal Starting-point Indicators taken from the front of table were used.

36. In September 1941, there was introduced the new system of SHA numbers, SCANOs and LN numbers designed to reduce and simplify book correction.

37. On the 1st October, 1941, the "Left and Right" recoding procedure, hitherto not used with the Auxiliary Vessels Tables was made effective for all three Area series of these tables. It was not, however, used with the special Western Approaches situation reports edition (see para.35).

38. From the 1st October 1941, authority was given to use plain-dress procedure with Auxiliary Vessels Tables; messages had, however, to be recoded entirely from right-hand pages.

39. On the 15th October, 1941, the old type of call signs and Delivery Groups published in two separate books - S.P.02218 War Call Signs (changing every two months) and S.P.02198, Delivery Groups (changing fortnightly)- was discontinued and replaced by one combined publication (S.P.02396) comprising both call signs and Delivery Groups. From this date, Delivery Groups, but not call signs, were subject to a recoding process by means of a simple daily-changing letter-substitution table in S.P.02318. At this stage, the second

TOP SECRET

and third letters only were recoded, because recoding first letter would have involved possible confusion through using three-letter Delivery Groups identical with certain call signs and address groups used by the R.A.F. Since it had long been appreciated that a secure system of Delivery Groups for use with codress signals was a sine qua non to cypher security, this measure was a distinct step forward. The intention was that editions of the new publication S.P.02396, using recoded Delivery Groups, should change automatically once a month; this compared with unrecoded Delivery Groups from editions of the old series which changed fortnightly but editions of which had, in fact, often to remain in force for longer periods owing to compromise and distribution difficulties. Although an improvement, however, it was clear that from the security aspect the new system was by no means the ultimate answer; the fact that the first letter was not recoded was, of course, recognised as a particularly weak factor. From the 15th July, 1942, onwards, confusion with R.A.F. call signs no longer applied and from that date all three letters were therefore recoded. This remained the practice until the 1st February, 1944, when the system was replaced by an entirely new one.

40. In November 1941 a revised recoding procedure for One-time Pads was made effective; Starting-point Indicators were still transmitted undisguised, but provision was made for using all lines of groups in a pad and not always starting to recode a message on the first line of a new page.

41. By December 1941, the load of traffic on the general recyphering table (S.P.02175) rose to new high levels, and a general warning was issued to restrict use of the Tables as much as possible, and wherever practicable to use area tables or other systems instead. The general tables were at this time changing fortnightly and each edition was carrying nearly 150,000 Groups which (taking into account the "Left and Right" procedure) gave an average depth of about sixteen.

42. From December 1941 onwards, large scale use of One-time Pads became general as one by one the new series of Admiralty and Senior Officers "Out" pads were brought into force.

TOP SECRET

Thus by 15th December, 1941 S.Ps.02403, 02407, 02416 were in force.
by 1st January, 1942, S.Ps.02417B - 9 were in force.
by 21st January, 1942 S.Ps.02548 - 49 were in force.
by 1st February, 1942, Mediterranean and East Indies "Out" Pads were in force.

43. It was decided that with this greatly increased use of One-time Pads, the time had come when the disguised Starting-point Indicators should be introduced to replace the self-evident 0101, etc. The object was to render One-time Pad messages indistinguishable externally from messages coded by long subtractor tables, and so:-

(a) to prevent any inference being drawn by enemy from use of special One-time Pads and -

(b) to increase the general mass of traffic which the enemy would have to attempt to sort for analysis and hence indirectly improve the security of ordinary long-subtractor tables.

From the 1st January, 1942, therefore, One-time Pad Table Indicators were provided in S.P.02169, and the true page-line Starting-point Indicators was disguised by subtracting it from the numbered groups on the last page of the pad corresponding to first two digits of the table indicator. Pending production of revised Indicator Books incorporating One-time Pad Indicators, the right-hand columns of all pages of the Indicator Book were allocated as One-time Pad Indicators with double-letter significations. (This disguised system was not, however, effective with the Navy 2, 3, 6, and 20 series until a month later - the 1st February, 1942).

44. On the 1st January, 1942, Naval Code No. 2 was brought into force to replace No. 1 which had been effective since 20th August, 1940, and Naval Cypher No. 4 was brought into force to replace No. 2 which had also been effective from that date.

45. As stated earlier in this section, it had become apparent early in 1941 that many views previously held about the security of the long subtractor system required modification in the light of developments. The volume of traffic continued to increase alarmingly and it was clear that loads on individual editions could not be satisfactorily checked even by the most drastic accelerations in the rates of change, to which also there was a limit governed by production and distribution problems. Editions of all our tables were already being produced at the maximum rate possible, but looking ahead it seemed

TOP SECRET

unlikely that we should ever be able to change editions faster than four times a month as an absolute maximum, and even this promised eventually to be too slow. Apart from this, we were, with the long-subtractor type of Table, always faced with the danger of peak traffic levels at certain periods; often at most dangerous times such as those immediately preceding and during important operations. With the long-subtractor Tables which remained in force for periods of from a week upwards, it was manifestly impossible to control traffic levels so as to avoid such peak depths, and it was obvious that some new and more secure method of using the subtractor recyphering system must, if possible, be found.

46. The Government Code and Cypher School had, in 1941, given close attention to this problem, and by the beginning of 1942 had evolved an entirely novel and very much more secure process known as the "Stencil Subtractor System". This system is now so well known that no useful purpose will be served in describing it in detail. It will suffice to say that initial trials, carried out in March 1942, to test the practical use of the new system, proved entirely satisfactory and production was started immediately ~~with~~ of Stencil Subtractor Tables for all series used with Naval Code and Naval Cypher. The outstanding advantage of the new system was to be the abolition of peak depths referred to above, since entirely new sets of recoding and recyphering groups were to be effective for every twenty-four hours.

47. In April 1941, a detailed analysis was ~~obtained~~ made to ascertain to what extent there was abuse of the system of haphazard selection of Starting-point Indicators. The analysis confirmed that code and cypher staffs still persisted in selecting indicators:-

(a) From right-hand pages.
(b) From the first few pages.
(c) Indicators which enabled re-coding to start near the top of a page.

A warning concerning the dangers of these practices was issued to the Fleet on the 17th April, 1941.

48. On the 1st May, 1942, consequent upon still higher traffic levels, further accelerations in the rate of change of certain editions were made effective. From that date, the heavily used Flag Officer's

TOP SECRET

table (S.P.02172) the general recypher table(02175 series), and the Area 1 and 2 general recyphering tables, changed 3 times a month, and an automatic monthly change was introduced for the Commander-in-Chief's Table (S.P.02171) and the World Wide Dangerous Waters Table (S.P.02350). A general warning was at the same time issued to the Fleet regarding traffic levels, and emphsis was laid on the need for authorities holding One-time "Out" Pads to use them in place of ordinary tables; also to restrict the volume of traffic in the Flag Officers Table to an absolute minimum. In order to reduce wear on the heavily used Mediterranean Area Tables, it was approved that Mediterranean Code "Out" Pads should in future be carried by ships in the Mediterranean, holding only a Dangerous Waters set of Books.

49. From the 1st June, 1942, it was possible to introduce an automatic monthly change of the Table Indicator Books (S.P.02169), thus implementing the policy for more rapid changes of this series which had been decided upon concurrently with introduction of the revised "double Indicator system" which became effective on the 1st September, 1941, (see para. 33).

50. Also from the 1st June, 1942, the U.S. Navy Department was supplied with the standard intra-R.N. editions of Naval Cypher and Naval Code and the general and area 1 tables, in order to relieve the wear on Naval Cypher No. 3 and its associated British- U.S. tables (for further details see special review on British-U.S. high-grade book systems). For a similar purpose, the Western Approaches Code and "Out" Pads were also issued to U.S. ships co-operating with Western Approaches Command vessels in convoy escort work.

51. On the 25th June, 1942, the inter-service cypher was brought into force as a high-grade inter-service system to replace the inter-departmental cypher and R.A.F. Station cypher. Until the 1st February, 1944, it was used with five-figure long-subtractor tables with five-letter (undisguised) starting-point indicators.

52. From the 1st July, 1942, consequent upon continued increases in the volume of traffic, still further accelerated programmes for world wide tables were introduced; thus, the general re-cyphering

TOP SECRET

table (S.P.02175)series) which was carrying 430,000 groups in June, 1942,(i.e. approximately 143,000 per edition) was changed four times a month. The general re-coding table (S.P.02176 series) which was carrying 575,000 groups a month,(i.e. approximately 192,000 groups per edition) was changed four times a month. This was the maximum rate of change found practicable for any long-subtractor table throughout the War.

53. From the 15th July, 1942, all three letters of the Delivery Groups were re-coded. This procedure continued until an entirely new system came into force on the 1st February, 1944.

54. On the 1st August, 1942, the new system of secrecy classifications incorporating "Secret Cypher", "Secret Code" and "Confidential Code" was made effective at Home. It became effective in all areas on the 1st November, 1942. The main object was to remove a proportion of work from overburdened cypher staffs by introducing a new "Secret" category ("Secret Code"): messages so graded were actually to be coded and decoded by ratings. At the same time, the additional classifications "Most Secret" and "Hush Most Secret" were established for classes of messages containing information of the highest degree of secrecy and which must never be handled or seen by ratings. From this date, the prefix AIDAC was abolished and the Prefix "Personal to be de-cyphered by an Officer specially selected by you" was introduced instead. An extensive glossary was for the first time provided showing the appropriate secrecy gradings for many subjects. With few exceptions, it was made permissable for messages graded "Secret Code" to be passed in plain language over the Defence Teleprinter Network. Hitherto, any message graded "Secret" had to be cyphered even when passed over secure home circuits, such as the Defence Teleprinter Network.

55. In August 1942, work started in MOSCOW on the production of an Anglo-Soviet Naval Cypher.

56. From the 17th September, 1942, the rates of change of two further series, the Area I general recypher/and recoding tables (S.P.02352 series - which carried 213,000 groups in August and the S.P.02355 series which carried 392,000 groups in August) were

TOP SECRET

accelerated to four times monthly. The rate of change of the general British-U.S. M. Table (S.P.02380 series which carried 218,000 groups in August) was also accelerated to twice monthly.

57. For Operation "Torch" (North Africa) landings in November 1942, special editions of area tables were used: this resulted in some distribution difficulties owing to some ships not having received them in time. In subsequent major operations, therefore, World-wide tables were used instead, special editions being set aside as necessary.

58. On the 1st December, 1942, a World-wide shore code recoding table (S.P.02475 series) was made effective; also a South Atlantic Series of Commander-in-Chief's "Out" Pads.

59. By December 1942 it had become apparent that the revised Indicator system introduced on the 1st September, 1941 (see para. 33) was not sufficiently secure to compete with the steadily increasing volume of high-grade book traffic. This could be attributed mainly to three factors:-

(a) On certain W/T services it had to be accepted as being clear to the enemy that much greater use was made of one, or possibly two, series of tables than of others. In consequence the enemy would assume, often correctly, that identical Starting-point Indicators appearing on that service referred to the same table. This had also the effect of assisting the enemy to classify Table Indicators in the S.P.02169 series.

(b) Despite repeated warnings to the Fleet, it was still not possible to overcome the human tendency to select "easy" Starting-point Indicators. As a result, frequent appearances of identical Starting-point Indicators were in fact likely to be the same "easy" ones taken from one and the same table.

(c) The standard "family" of Starting-point Indicators used for all tables must by then have become known to the enemy, thus defeating the object which it was desired to achieve when One-time Pads Starting-point Indicators were disguised in order that they should be indistinguishable from Starting-point Indicators used with long Subtractor Tables.

60. From the 15th December, 1942, a system of disguised Starting-point Indicators was therefore re-introduced for all Naval Tables except the daily sections of the Submarine Tables. The system, although simple, resembled the disguised procedure which had previously been effective from 20th January 1941 to the 31st August, 1941. The true Starting-point Indicator was disguised by subtracting

TOP SECRET

it from the numbered group on the last page of the table corresponding to the first two digits of the Table Indicator. This system remained effective for all Naval (except Submarines) tables until replaced by the Stencil Subtractor system in 1943 and early 1944.

61. In December 1942, it was decided that, pending the forthcoming introduction of the stencil subtractor system, a procedure should be made effective by which Admiralty and certain Commanders-in-Chief should have a One-time system available for communication with ships in any area who held Naval Cypher; this could not be implemented by any normal type of One-time Pad series. Special editions of the general (World-wide) re-cyphering table for Naval Cypher (S.P.02175 series) were therefore set aside for exclusive use, by Admiralty and the Commanders-in-Chief concerned, as a One-time "Out" table. The editions were divided into sections, so many pages being allocated for use by each originator. The normal disguised Starting-point Indicator system applicable to One-time Pads was used together with Table Indicators specially allocated. The first of these special tables was brought into force on the 18th December, 1942, and further editions were subsequently used until the stencil subtractor system had become generally effective towards the end of 1943.

62. In January 1943, there was evolved and promulgated two new systems for using One-time Pads without a basic book; one, using normal figure pads from which to subtract letters of the plain language converted into digits; 01 = A, 02 = B, etc; the second system provided for use of specially prepared five-letter group pads under which the letters of the plain language text were written and then coded by means of a simple letter over letter substitution table printed inside the cover of the table. Extensive and successful use of these systems, but more particularly of the second method, was later made in the conduct of various hazardous operations in circumstances where the risk of losing a basic cypher or code book could not accepted. The chief disadvantage of both systems was, of course, the absence of a basic vocabulary book, and hence the need for letter by letter coding and recoding, resulted in a tedious process and substantly increased the number of groups required to code a given length of

TOP SECRET

text. Later, this disadvantage was largely overcome by use, in particularly hazardous operations, of a long-since obsolete four-figure book, "British Cypher No. 5", together with 2, 3, 6 or 20 way series of One-time Pads. This, of course, provided complete security in spite of the known compromise of the basic cypher.

63. In the same month (January 1943), resulting from an impass with the Russians, work on the Anglo-Soviet Cypher ~~System~~ ceased / in MOSCOW, and the Officer from Admiralty who had been appointed to work with the Russians in MOSCOW returned here to complete his work in the form of a British-U.S.-Soviet Cypher. The manuscript of the new book was completed in March 1943 and the cypher went into production. It was finally completed and in course of distribution by July 1944. The Cypher had, of course, been prepared with a view to its introduction in the event of hostilities breaking out between RUSSIA and JAPAN. In the final event it was never used.

64. By the end of 1942, the volume of Naval traffic carried by subtractor tables and machine cypher (Typex) had risen to nearly 8,000,000 groups a month. In spite of changing the more heavily used tables as frequently as four times a month, it was clear that with this huge load of traffic, some parts of our General and Area Tables might well be reconstructed by the enemy, and messages or portions of messages might be read by him after a time-lag varying perhaps from a week to several months from the dates of origin. On the 23rd January, 1943, a general warning in these terms was signalled to all Flag Officers, and emphasis was laid on the need for maximum use of machine cypher and One-time Pads in place of long-subtractor tables. It was stressed that every unnecessary signal must be eliminated and that very particular care must be taken in drafting signals which cannot be made in a one-time system; the latter precaution applied particularly to signals whose texts might disclose future operational intentions.

65. It is of interest to note here, that in the signal referred to, Flag Officers were informed that an ordinary subtractor table of 100 pages (15,000 groups) could safely carry 30,000 groups, when using

TOP SECRET

the "Left and Right" procedure, but that after this figure it "becomes progressively weaker". In point of fact, later experience was to show that such a load was by no means safe, since even allowing for 20% of messages being recoded on left-hand pages, it would result in an average "depth" of well over three on the right-hand pages, and therefore peak depths very substantially higher. At that time, virtually all our widely held tables, were loaded well beyond this "safe" limit of 30,000 groups. Introduction of the new stencil-subtractor system had by now therefore become a matter of extreme urgency. There had, however, been numerous technical difficulties to be overcome in connection with this new system, both with regard to the stencil device itself and the type of subtractor table for use with it; the latter presented numerous production problems not encountered with the normal type of long-subtractor table. Production and distribution of the components for the new system had however been pushed ahead as a matter of first priority, and the scheduled date for introduction of the first stencil-subtractor tables was the 1st July, 1943.

66. Naval Code No. 3 was made effective on the 1st March, 1943, to replace No. 2 which had been in force since the 1st January, 1942. Edition No. 3 was the first of new editions of this book incorporating a number of security improvement made as a result of war experience; for example the system of self-evident "switch" groups was abandoned, and numerous alternative groups were provided for the more commonly used words and phrases. The latter was a practice which had been in force many years previously, but had been dropped as it was thought to be no longer necessary when the long-subtractor system of recyphering was introduced.

67. Meanwhile, the security importance of the basic book itself had long since re-established itself after a period when the security of the basic groups was considered secondary in importance to that of recyphering groups, and steps had been taken greatly to accelerate the production of new editions of both Naval Cypher and Naval Code. Accelerated production was facilitated by making the lay-out of both books identical. It was decided that in future every endeavour should

be made to change editions of Basic Books at not more than six-monthly intervals; this programme was adhered to in the main until the end of hostilities.

68. In May 1943, a new system was evolved for the distribution, use and identification of recoding and recyphering tables used with Naval Cypher and Naval Code. Experience had shown that the system of Area tables which had been introduced first in October 1940, and which by early in 1941 had become effective generally, whilst it achieved the object originally intended, i.e. minimised risk of general compromise of Fleet communications and reduced wear on World-wide Tables, nevertheless had certain disadvantages in as much as difficulties frequently arose through ships moving from one Area to another not being in possession of the tables current in the new area; a measure of doubt was often present, therefore, in the mind of originating authorities as to whether ships on passage were in fact holding all the necessary publications. In theory the practice should have worked satisfactorily, in as much as the requisite tables should be embarked before a ship entered a new area; in practice, however, this was often not possible, either because adequate stocks of the necessary ~~Starting-point Indicators~~ SPs were not invariably held at the focal points concerned, or else ships proceeded at such short notice that timely embarkation of the tables was not possible. A further difficulty arose by reason of fact that different Area Tables of the same type were all identified in the Indicator Book by the same letters, thus, on occasions, necessitating a procedure of trial and error before determining the correct table required to decode a message. This new system overcame these difficulties in as much as it provided for World-wide distribution of the main Area 1, 2, and 3 recoding and recyphering Tables hitherto distributed within their respective Areas only, whilst retaining Area distribution only for the Auxiliary Vessels, Dangerous Waters, and Submarines tables. The three main Area Tables, although in future to be distributed world-wide were to be used only by Originators in the Area concerned. This satisfied the requirement for limiting the traffic in these tables mainly to the Areas for which they

TOP SECRET

were provided, whilst permitting messages recoded by them to be decoded by ships in all three Areas.

69. Concurrently with the introduction of this new system, revised and greatly enlarged editions of the Table Indicator Book (S.P.02169 series) were to be made effective and each individual series of tables was in future to be identified by its own distinctive single or double letter. Single letters were reserved for the tables in world wide use and double letters for the tables distributed only within each of the three Areas.

70. In June 1943, after discussions with Admiralty, the Australian Commonwealth Naval Board produced, and put into use, four local series of long subtractor tables for use with Naval Code and Naval Cypher, thus re-introducing use of Area Tables in the Pacific, which had been discontinued in 1942 when Area 3 was re-defined as comprising the Indian Ocean only.

71. In June 1943, when introduction of the stencil-subtractor system of recoding and re-cyphering was imminent, the Government Code and Cypher School conducted a test to ascertain the probable margin of security afforded by the new method. The test was conducted on the assumpton that the stencil-subtractor system had been compromised to the extent of the enemy having captured a basic Code and Decode, together with the stencil mask and (obsolete) stencil-subtractor tables, and so were completely aware of the procedure. For the purposes of the test, the ~~seven~~ personnel conducting it were supplied with 500 recoded messages, all but 50 of which were known to them to have been coded from the same basic book Naval Code using one and the same stencil subtractor Key Sheet; they were also supplied with the stencil mask and copies of the basic Code and Decode used. The 500 messages averaged 40 groups each; the test was therefore carried out on approximately 20,000 recoded groups. It was, generally speaking, very satisfactory in as much as the greatly improved security provided by the new system was proved. Even with a double substitution indicator system, however, the conclusions were that complete security could not be guaranteed, after the enemy were in possession of the basic book and the stencil mask, if the number of messages recoded from the same Key sheet exceeded a hundred.

TOP SECRET

It was considered, however, that, with the number of messages under five hundred (approximately 20,000 groups), solution by any known cryptanalytical process would be a matter of great difficulty and would require exceptionally favourable circumstances. It was recommended that, to achieve complete security for traffic ranging from 300 up to 500 messages recoded on the same sheet, the single substitution indicator system originally devised should be modified to preclude level starting depths. This modification involved the original single conversion (substitution) plus a second process of subtracting from the result of the first process a four-figure group from the conversion table determined by the first two digits of the selected Table Indicator.

72. The first Naval Stencil-Subtractor Table became effective on the 1st July, 1943. Subsequent Stencil-Subtractor Tables were brought into force on the first day of each succeeding month of the year, and, by the 1st January, 1944, all tables were Stencil Subtractor ones, except the Area 3 Submarines Table which transferred to Stencil Subtractor on the 1st March, 1944, and the Naval Shore Code tables which transferred on the 1st January, 1945. Apart, possibly, from introduction of Machine systems, this represented the greatest advance hitherto on the road to high-grade cypher security. The nightmare of peak traffic volumes and depths on long subtractor tables ceased, and the average daily traffic on the various Stencil-Subtractor Tables was limited to well below the daily 20,000 groups (500 messages) which had been taken as the accepted maximum for the purposes of the test. Unfortunately, however, it was not practicable until the 1st January, 1944, to make the Stencil Subtractor system effective for the British-U.S. recyphering tables, the security of which remained the greatest cause for concern (see separate review on Naval Cypher No. 3 - the British-U.S. Cypher).

73. On the 1st June, 1943, a new edition of Naval Cypher (No. 5) was brought into force to replace No. 4. which had been effective since the 1st January 1942, and on the 10th June, 1943, the same edition replaced Naval Cypher No. 3 as the standard British-U.S. Cypher.

TOP SECRET

From this latter date, one edition only of Naval Cypher was used both for intra R.N. and British-U.S. communications. The new edition (No.5) was similar in lay-out to the new edition of Naval Code (No.3) which had become effective on the 1st March, 1943, and it incorporated the same security improvements as the latter (see para. 66).

74. In June 1943, special communication arrangements were made for the "Monster" Troop-carrying liners. From this date onwards these liners were provided with a Major War Vessels establishment of Codes and Cyphers.

75. In July 1943, analysis of traffic revealed that neglect was still widespread in regard to the security precautions necessary when transmitting the same message in different cyphers, and a further warning was issued to the Fleet on the subject. Analysis also disclosed the extensive use of stereotyped phraseology, particularly at the beginning and end of messages, and special instructions on this point were issued to the Fleet together with guidance on the type of wording to be used.

76. On the 1st July, 1943, an increased in the security of Lettered Co-ordinates was effected by introducing a fortnightly (in place of monthly) change of editions.

77. On the 1st September, 1943, there was made effective for general fleet use a system of Fleet R/T call signs which replaced the procedure hitherto in force by which R/T call signs were provided by local allocation. The new system provided for R/T call signs being associated with ships' pendant numbers. A degree of security was achieved by using a daily changing index number to be added or subtracted from the pendant number.

78. In October 1943, production was put in hand of two series of Stencil-Subtractor Tables for British-U.S. use in the Pacific. These were later distributed, but were in fact never used as other arrangements were made in that theatre.

79. On the 1st November, 1943, welcome relief was achieved for the overloaded British-U.S. Tables by introduction of the Combined Cypher Macine in the North Atlantic (see also separate review on

TOP SECRET

(British-US communications).

80. In January 1944, analysis of traffic brought to light further irregularities in the handling of Naval cypher and Naval code. Excessive and unnecessary use was being made of certain groups for syllabic spelling. The requisite warning was issued to the Fleet.

81. On the 1st February, 1944, the existing system of Call Signs and Delivery Groups for major war vessels was replaced by an entirely novel and much more secure system. Call Signs and Delivery Groups remained incorporated in the same book, but two parts were provided. The first part contining names of ships and authorities, each with one or more five-figure groups. The second part, changing monthly, contained the three-letter call signs and delivery groups associated with the five-figure groups in Part I. Security for Delivery Groups was achieved by provision of daily changing index numbers to be added to the five-figure groups in Part I before selecting the appropriate Delivery Group from Part 2. Call Signs were not subject to addition of the daily index figure; they were however made subject to it after the defeat of Germany in order to achieve additional security for the increased volume of plaindress signalling. This new system was satisfactorily both from the practical handling and security points of view and is still in force. It could not, however, be made applicable to Auxiliary Vessels owing to shortage of three-letter groups: the Auxiliary Vessels Call Sign System had therefore to continue in force. The latter system is necessarily an insecure one and has the added disadvantage of distinguishing as such all messages recoded by means of the Auxiliary Vessels Tables.

82. By agreement with the U.S. Navy Department, the Admiralty cypher "Out" Pad (S.P.02416) was, from the 23rd February, 1944, shared by Navy Department and issued to all U.S. as well as H.M. Ships in the North Atlantic holding the "S" recyphering table. Each edition of this Pad was used concurrently by Admiralty and Navy Department, the existing security depth of two over certain portions being acceptable.

TOP SECRET

83. On the 15th March, 1944, there came into force a revised system of secrecy classifications, resulting from British- U.S. discussions in Washington. The revised arrangements provided for discontinued use of the classifications "Secret Cypher", "Secret Code" and "Confidential Code", and their replacement by "Secret", "Confidential" and "Restricted" respectively. The term "Most Secret" was also replaced by "Top Secret". Sofar as the security aspect of Naval Communications is concerned, the changes had little effect, but since the revised instructions were applicable to all Services of both nations certain minor changes in Naval procedure were inevitable. Amongst these was the instruction that, in future, messages graded "Secret" might (with few exceptions) be passed in plain language over secure line circuits. Previously, this had been applicable to "Secret Code" but not "Secret Cypher."

84. In April 1944, with Operation "Overlord" pending, instructions were issued designed to safeguard the security of the Fleets' communications as a whole should copies of codes and cyphers be lost in the course of "launching an amphibious operation from the U.K. against enemy occupied territory." Numerous codes and cyphers normally carried by ships in home waters were withdrawn and reserve editions of those codes and cyphers which were retained were reduced to a minimum. Special instructions were also issued respecting the destruction of S.Ps. in an emergency.

85. From the 15th April, 1944, onwards there were made effective numerous specially prepared cyphers for use only in the European Theatre of operations; the assumption being that compromise of S.Ps. during the assault on the Continent was likely, and it was important, therefore, that Fleet communications should not be prejudiced, by such compromise.

86. Experience in previous large-scale operations, notably "Torch" had showed that for simplicity sake the normal naval re-coding and re-cyphering tables should, so far as practicable, remain effective for use during major operations. For Operation "Overlord" this practice was therefore adopted but a special series of One-time Pads were issued, and one-time systems were used throughout for much of the more important signalling. In point of fact

TOP SECRET

no compromise by loss was sustained by any of our high-grade systems during the assault on the Continent, and special arrangements made worked smoothly.

87. For operation "Overlord" special Books of British-U.S. callsigns were produced and used.

88. Further to increase security of the stencil-subtractor system, a ~~table~~ double indicator conversion procedure was made effective on the 1st May, 1944 and has remained in force since then.

89. Starting from the 1st June, 1944, the revised system which involved changes in distribution and identification of Tables became effective and was completed by the 1st August, 1944.

90. Re-cyphering Tables for the Inter-Service ~~tables~~ Cypher transferred to the stencil subtractor system ~~from was used.~~ on 1st June 1944.

91. On the 1st July, 1944, the new system of call signs and delivery groups became effective for British - U.S. use, replacing the old call signs in S.P.02378 which had been in force since America entered the War.

92. On the 1st August, 1944, the basic Naval Codes and Cyphers changed. Naval Code No. 5 and Naval Cypher No. 7 came into force. Both remained in force six months, until the 1st February, 1945.

93. In 1945, when the B.P.F. adopted U.S. communication methods, British high-grade systems were almost entirely removed from that Fleet. Apart from a very few tables retained for use by ships not equipped with machine system or as a stand-by for the latter, all high-grade R.N. systems were withdrawn.

94. From the 1st March, 1945, Inter-Service Cypher was re-cyphered by a new and smaller type of stencil-subtractor Tally used in conjunction with the Army Brigade stencil-subtractor frame.

95. In April 1945, detailed instructions were issued for extension of plain language on defeat of Germany. One of the relaxations which became effective after the defeat was plain language reporting of movements of merchant ships, other than transports, in non-combat areas. Since it was not permissable, however, for Reporting Officers

TOP SEC

in neutral territory to use plain language for this purposes, a special edition of World-wide Shore Code Table was provided for their special use, so as not to compromise normal editions which would otherwise be the case if departures from one port were reported in plain language and arrivals in the next port, in code.

TOP SECRET

PART I - SECTION A - 2 - HIGH-GRADE-MACHINE SYSTEMS.

TYPEX. The Typex, Mark II, Cypher (Coding) machine was originally developed by the Air Ministry for R.A.F. communications, and was first used in 1937 between the Air Ministry and Headquarters of R.A.F. Home Commands.

2. In 1938, five machines were ordered for Naval trial. These were received in the late summer of 1939, and by the end of the year were in operation in Admiralty and at Malta and Gibraltar. The drums then used comprised the original set of five black Mark II in use by the R.A.F. and also by the Army, who meanwhile had acquired a number of machines. Special naval machine settings (S.P.02305) were used for Naval communications.

3. The tests proved successful, and in May 1939 a further 50 machines were ordered for Naval use. After the outbreak of the War, another 575 Machines were ordered for the Navy, the intention being to equip all Major War Vessels and shore Coding and Cypher Offices. The machines were at this time also effective for inter-service traffic, using the Army Home Machine Setting Key since inter-service Keys had not yet been produced. Further orders for machines to meet Naval requirements were placed at intervals throughout the war up to a total of 3,302. Of this number, some 2,300 had been delivered by the end of hostilities.

4. By the middle of 1940, the machines had been installed in a considerable number of shore Coding and Cypher offices and were carrying a large volume of Naval high-grade traffic. In August of that year, revised Naval Machine Setting Keys were made effective; these comprised two series; one (S.P.02325) for Cypher traffic and one (S.P.02326) for Code traffic. Up till 2nd September, 1940, the Machine Setting remained constant for one week, but from that date daily changes were made effective in view of the ever increasing volume of traffic.

5. On the 1st June, 1941, two additional drums were added to the original set of five; these comprised two red drums from the set of five red drums which had been wired for use in addition to the five

TOP SECRET

black ones referred to earlier. From this date, all Machine Setting Keys provided for use of seven drums.

6. On the 1st ~~October~~ July, 1941, the Army Home Settings were discontinued for inter-service use, and were replaced by the first edition of the Inter-Service General Key (S.P.02347 series). A Special (Flag Officers level) Inter-Service Key was added on the 1st October 1941 (S.P.02348 series).

7. Up till the end of October, 1941, no disguised message setting procedure was used. The actual initial setting of the drums was transmitted as the first and last groups of the message or message section. Naval Code X traffic was distinguished as such by the operator chosing a message setting with an initial letter between A and M inclusive; Cypher X traffic by the letters N to Z inclusive. Use of the Inter-service Keys was denoted by a self-evident prefix to the coded groups. Message sections were limited, for security reasons, to 60-70 groups, after which a new message setting was chosen. Sections were separated by groups of five Q's.

8. On the 1st November, 1941, there was brought into force the first edition of a Naval Message Settings Book (S.P.02349(1)). This included appropriate Disguised Message Settings for all Naval and Interservice Machine Setting Keys. These disguised settings not only gave the appropriate true setting to which drums must be set before starting to encypher a message, but also denoted the Key List used. From this date, therefore, the practice of operators choosing their own settings, as described above, ceased. Introduction of this Book also resulted in discontinued use of the separate sign of five Q's for message sections, since the disguised settings were readily distinguishable as such. Naval Commanders-in-Chief and Flag Officers' Key Lists were made effective for the first time on the 1st November, 1941.

9. Meanwhile, as an added security measure, a plugboard scrambling device had been evolved, and in November 1941 these units started to be fitted to machines, although they were not brought into force until later.

TOP SECRET

10. In December 1941, Typex machines were supplied to the American Navy as an additional medium of high-grade communication between R.N. and U.S.N. shore authorities on the North Atlantic seaboard. At this time, however, the Americans were not supplied with the normal R.N. Key Lists but with a special Key List (S.P.02387 series) for Limited Combined Naval Use only. The normal Mark II set of seven drums, referred to earlier, were used with this Key List.

11. It became apparent, late in 1941, that requirements for these machines in shore Code and Cypher Offices was so large that the supply was inadequate to complete also with a programme of equipping seagoing ships. Moreover, use of Typex for shore-ship and ship-shore work could be looked upon as a relatively long-term policy only, since it was unacceptable, from the W/T security standpoint, to introduce such a distinctive system peacemeal in H.M. ships.

12. Excepting those Machines issued to Fleet Flag-ships, all machines held by seagoing ships were therefore withdrawn and used to supplement the supplies for shore Code and Cypher Offices. No further machines were issued to seagoing ships throughout the War except (later) modified machines for use as C.C.M. An exception was made in the case of Landing Ships Headquarters.

13. By the 1st March, 1942, fitting of plugboard units had advanced sufficiently for Naval plugboard Setting Keys (S.P.02426 series) to be made effective on that date for a proportion of Naval Cypher X traffic. Use of the plugboard and Key was confined to known holders and was distinguished by the self-evident prefix FIELD.

14. In order to divert a greater proportion of traffic off the heavily used British-U.S. recyphering tables, it was decided, in the Spring of 1942, to issue all U.S. holders of Typex with the standard Naval Cypher X and Code X Keys (S.P.02325 and 02326 series) in addition to the special Key referred to in paragraph 10 above. This arrangement became effective on the 1st June, 1942.

15. By July 1942, the total Naval traffic carried by Typex had

TOP SECRET

increased to 1,900,000 groups a month which was approximately one third of the whole volume of Naval traffic.

16. On the 15th September, 1942, a separate Inter-service Message Setting Book (S.P.02456 series) was introduced to take the place of the Inter-service message settings hetherto incorporated in the Naval book (S.P.02349).

17. It had become apparent during 1942 that the steadily increasing volume of Naval Typex traffic called for provision of separate Naval drums for use in place of the original standard set of 7 Mark II drums. (For example in December 1942 Naval Typex traffic amounted to 2,216000 groups, which was still approximately one third of all Naval traffic).

18. Arrangements had therefore been made with the Air Ministry to wire two separate 7-drum sets of Naval drums, one for Cypher X and one for Code X. These were distributed to all Naval holders of Typex during the latter part of 1942 and early 1943, and the Cypher X drums (which were completed in advance of the Codex ones) were brought into force on the 1st February, 1943, for all Naval Typex traffic. The Naval Codex drums followed on the 1st April, 1943, and from that date were used exclusively for Naval Codex traffic. The original Mark II set of seven drums remained effective for Inter-service traffic only.

19. Resulting from a review by the Government Code and Cypher School of the security of Typex, it was approved as from the 17th September, 1943, for message sections to be increased up to approximately 150 groups when plugboard settings were used. This affected the bulk of Naval Cypher X traffic, which by this time was being encyphered using plugboard Keys. Naval Codex traffic was not affected, as Codex Plug-board Keys were not then in force due to a continued shortage of Plugboard units resulting from manufacturing difficulties.

20. On the 29th December, 1943, following a further review of Typex security, which amongst other things showed that this system was particularly vulnerable to cryptographic attack from sterotyped beginings, a revised procedure for concealing the start of the text was brought into force. From this date, the first ten to fifteen words

TOP SECRET

of the subject matter were buried in the text, in addition to the address.

21. By December, 1943, the volume of Naval Typex traffic had increased to over three million groups monthly; this practically equalled the volume carried by Book systems.

22. As an additional measure of security, an entirely new indicator system was made effective from the 1st February, 1944. This involved the use of two, instead of one, disguised message setting, and determination of the "true encypherment setting" by a process of encyphering the true setting of the second indicator with the machine set to the reading of the first indicator. The first indicator served also as an indication of the Key List used. This process virtually overcame the problem of presented depths.

23. The revised procedure was, of course, a considerable added complication which slowed down the process of encyphering and decyphering a message; this was to some extent mitigated, however, by certain latitude which was now permitted over Message Sections. Thus, the procedure by which new inidcators were required for each message section was discontinued, and instead the practice was adopted by which message sections were once again distinguished by the self-evident group of five Q's with the added proviso, however, that after each such group the right hand drum must be rotated one place before encyphering was continued.

24. The Typex system was known to be particularly vulnerable to attack from "cribs", i.e. the possession by the enemy of knowledge of the plain-language version of a message in Typex. Concurrently, therefore, with the new Indicator procedure described above, there was introduced an added complication in the form of the random use of the letter-shift key, thus breaking up the relationship between the cyphered version as transmitted, and the plain language words of the message.

25. In April 1944, the cyclic procedure was introduced as a security measure in the cyphering of short messages which, by reason of their brevity, were unsuited to the "buried address" procedure.

26. In anticipation of the Assault on the Continent, special Typex Inter-service Key Lists and Message Settings Books, for use exclusively in the European Theatre of operations, were made effective on the 15th April, 1944.

27. By May 1944, the distribution of plugboard units throughout the three Services had sufficiently advanced to permit the Inter-service Plugboard Key (S.P.02427 series) being made effective from the first day of that month. The self-evident prefix FIELD continued to be used to denote messages encyphered using the Plugboard KEY.

28. Use of the special British-U.S. Key (S.P.02387 series) was discontinued on the 31st May, 1944, and from then onwards all British-U.S. Naval Typex traffic was carried on the two standard Naval Codex and Cypher X keys.

29. The letter-shift procedure (para. 24) which had been effective since the 1st February, 1944, was on the 14th September, 1944, modified, for practical reasons, to a "Figure shift-letter shift Procedure".

30. Up till October 1944, the interservice drums had consisted of the original seven Mark II Typex drums, but there had been uncertainty whether or not one or more of these drums had been physically compromised; moreover they had carried a vast load of traffic since first put into service. An additional three drums for inter-service use had therefore been wired, and these were brought into force concurrently with new seven-drum inter-service Key Lists on the 1st October, 1944.

31. In order to provide for expansion in the number of different Key Lists in use, the Indicator system used with the inter-service Message Settings Book was modified from the 1st October, 1944 onwards. From that date the Key List used was indicated by the initial letter of the true setting corresponding with the First Indicator. (The same procedure was applied to Naval Message Settings from the 15th June, 1945).

32. By December, 1944, the volume of Naval X traffic had easily surpassed the total of traffic in Book systems (4,400,000 groups monthly as opposed to 3,600,000).

TOP SECRET

33. Further investigations into the security of Typex proved that use of the Plugboard did not chieve all the results originally anticipated. It gave protection from one method of attack only (cataloguing): this protection could, however, be achieved equally well by use of one series only of Plugboard Keys, and with the plugboard setting changing monthly instead of daily as hitherto. From the 15th March, 1945, therefore, daily changing plugboard settings were abolished, and pending introduction of a Universal plugboard Key with two series of settings (one for use only with the most heavily used machine setting Keys), all plugboard settings were chosen from the inter-service plugboard Key, the daily settings being retained in force for a month.

34. Further experience had also showed that, with the revised Indicator procedure now in force, message sections could be increased up to 200 groups whether or not a plugboard was used. This increased length of sections became effective from the 15th March, 1945.

35. Analysis of typex traffic early in 1944, disclosed that a significant number of corruptions were caused either by complete failure on the part of the drums to rotate, or by drums rotating at incorrect intervals. This was of course a matter for serious concern from the security aspect, and special instructions were issued in June 1944 which, apart from dealing with the mechanical aspect, stressed the security precautions necessary in asking for, and giving, checks and repetitions of messages which were thought to be corrupt due to faulty drum rotation.

COMBINED CYPHER MACHINES.

36. Since early in 1942, the U.S. Navy Department had been experimenting with production of a Combined Cypher Machine to take the place of the British Naval Cypher as a limited-combined Naval high-grade system. The Americans were firmly wedded to the idea of such a machine because virtually all their own high-grade traffic was in machine cypher and they disliked having to use the British book system; moreover, they shared with us the concern over the security of the heavily used British-U.S. recyphering tables, and like us, were anxious to introduce a sounder system as soon as possible, particularly in the vital North Atlantic Area.

37. The problem was to design an adaptor which, when fitted to the British Typex Machine and to the American ECM (Electrical Cypher Machine) would enable both types of machine to be used for inter-communication.

38. By October, 1942, Navy Department experts had designed such an Adaptor for the Typex machine, and the prototype was brought to London by them for demonstration and tests. The tests were successful and, with a few small modifications, incorporated as a result of the test, production of 4,500 of these Adaptors to meet the requirements of all three British Services was in hand in America by the end of the year.

39. It was clear, however, that conversion of Typex Machines into C.C.Ms, Mark III (which was to be their designation when fitted with the Adaptor) would be a somewhat lengthy process, since considerable modifications were necessary to the basic Typex machine itself before the adaptor could be fitted and used; moreover, deliveries of Typex Machines for all three British Services were still far short of requirements. In order therefore to accelerate the date when C.C.M. could be made effective in the North Atlantic for Convoy Escort communications, the Navy Department meanwhile designed and perfected a number of self-contained C.C.Ms. (C.C.M. Mark II) for issue to H.M. and H.M.Canadian ships engaged on Convoy escort work in the North Atlantic. Deliveries of these machines started in May 1943, and ships concerned were fitted with them as far as possible. By July 1943, the Adaptors for Typex started to arrive from U.S.A. and the conversion of Typex machines into C.C.M. Mark III proceded apace.

40. By the 1st November, 1943, sufficient Mark II and Mark III machines had been fitted to enable the C.C.M. system to be made effective in the North Atlantic. Some 250 of H.M. ships and H.M. Canadian Ships had by that date been equipped.

41. The C.C.M. was initially used, therefore, for limited combined Naval traffic only. The Keys used comprised one General Naval Key held by all C.C.M. ships and authorities, and one Key

TOP SECRET

limited to Flag Officers only. Considerable discussions took place with the Americans over external indicators to be used to denote Key Lists. It was the original American view that fixed indicators would suffice, but Admiralty pressed for introduction of a system of changing indicators in order to disguise Flag Officers traffic from General traffic. A system of Rotating Indicators was therefore evolved and made effective from the outset. This consisted of daily-changing lists of external indicators applicable to each Key List.

42. In the first month it was used (November 1943), C.C.M. Traffic originated by British holders exceeded 100,000 groups. The volume of traffic increased, progressing, month by month.

43. The fitting of C.C.M. had so far progressed, that by the 31st December, 1943, the system was made effective for Limited Combined Naval use also in areas outside the North Atlantic. By the 15th April, 1944, the other two British Services had installed sufficient C.C.Ms. to enable the system to be made effective for combined (five services) use. Three Key Lists were introduced initially; a General, a High Command and, in view of the forthcoming Assault on the Continent, a special series for use in the European Theatre of operations only.

44. A special edition of the American "Strip Cypher" was introduced from the 15th May, 1944, as a standby Combined (five services) system for use in the event of breakdown of C.C.M.

45. By June, 1944, C.C.M. Naval traffic originated by British holders had had increased to over a million groups monthly, and by December, 1944, to over 1,300,000 groups.

46. By the 31st December, 1944, 1,220 Naval Typex machines had been modified as C.C.Ms. Mark III, and the C.C.M. system was firmly established as the main Combined and Limited Combined Naval high-grade system.

47. The security of C.C.M. was the subject of constant investigations both here and in the U.S.A, and on the 1st January, 1945, a revised and more secure system of internal indicators was brought into force and has remained effective since then. Large numbers of additional Key Lists, and further sets of code wheels for use with them, were also made effective during the course of 1944 and 1945. From mid-1944 onward-

TOP SECRET

first priority was given to the equipment of the British Pacific Fleet with C.C.Ms, and by February 1945, when the B.P.F adopted U.S. communication methods, virtually all Major War Vessels of that Fleet had been equipped with C.C.M.

TOP SECRET

PART I - SECTION A - 3.

SPECIAL REVIEW OF SECURITY OF NAVAL CYPHER AS A BRITISH-U.S.

HIGH - GRADE SYSTEM.

It has been thought desirable to append this special review, because the degree of security of British-U.S. high-grade communications from the date of entry of America into the war on the 7th December, 1941, until the 31st, December, 1943, when the long-subtractor system of recyphering was discontinued, was during the major part of that period a matter of grave concern to the cypher security departments both of the Admiralty and of the U.S. Navy Department. Part 2 of this Review provides confirmation that our fears on this score were justified.

2. As early as 1940, it became apparent that provision must be made for a secure British-U.S. high-grade cypher, not only against the ultimate eventuality of the Americans making common cause with us against Germany, but for possible use with the Americans in the Atlantic even before then, since British-U.S. co-operation over Convoy protection work in the North Atlantic was daily becoming closer in the face of American determination to defend shipping in West Atlantic waters from the growing depredations of U-Boats set with the task of cutting off supplies of American material to Britain.

3. Resulting from staff discussions with Navy Department in 1940, it was decided, therefore, that Admiralty should set aside an unused edition (No.3) of the British Naval Cypher as a British-American Naval Cypher, and should produce two series of Recyphering Tables for use with it. These were the S.P.02379 series ("H" Recyphering Table) for use by Flag Officers of both Navies, and the S.P.02380 series ("M" Recyphering Table) for general use by all British and American major war vessels in all areas. No alternative system was at the time available. The Americans had nothing comparable to offer us, since they used Machine Cypher (The E.C.M.) for their own high-grade Naval communications, and, even had they been willing to share with us the closely guarded secrets of this system (which they were not, and never had been), there would have been no possibility for a long time ahead of providing sufficient machines to equip H.M. Ships, let alone adequate time to

TOP SECRET

instal~~l~~ them in the latter and to indoctrinate cypher staffs in the use of a machine cryptographic system, which at that period of the War was entirely novel to us except in certain shore headquarters where the British Typex Mark II Cypher (Coding) machine was in operation.

4. Naval Cypher No. 3. was a normal edition of the standard four-figure British Naval Cypher, and the H and M recyphering tables provided for use with it were the standard type of British Naval long-subtractor tables then in common use, each edition comprising 15,000 groups with associated Starting Point Indicators.

5. Naval Cypher No. 3 and these two series of Tables were therefore distributed early in 1941 both to H.M. and to U.S.N. ships, and were actually made effective on the 16th June, 1941; i.e., nearly six months before Pearl Harbour. The Americans were also supplied with our Table Indicator Book S.P.02169 series. Very little use was however made of the cypher in the early months, traffic being limited to a small volume of signalling, mainly between shore Naval Headquarters on both sides of the Atlantic. Introduction of the system at this stage served, however, a useful purpose in affording the Americans practice in the use of book cypher and the long-subtractor system. It was not until October 1941 that there was any appreciable traffic, and not until America entered the War in December 1941 that traffic figures in the general (M) recyphering table showed a heavy increase. The chart accompanying this section illustrates the load of traffic carried by British-U.S. recyphering Tables from the 1st October 1941 until the 31st December, 1943, and also the average "depth" of traffic carried at various times by individual editions of these Tables.

NOTE. It should be emphasised that the figures shown in ~~the~~ the chart represent traffic originated by British ships and authorities only. Like figures in respect of American originated traffic are not available, but it may be assumed these represent some third of the British figures.

The actual depths are therefore correspondingly higher than those shown. No account can also be taken of peak depths at particular periods during the life of a table.

6. British and American cryptographic experts have always been in general agreement over the security margin afforded by the long-subtractor system of recyphering. In 1941, however, when these British-U.S. Tables were introduced, experts of both nations held the view that this system afforded a greater margin of safety than was later proved to be the case. Since then, new methods have shown that the long-subtractor table is far more susceptible to attack than was originally thought, and that reasonable security against expert cryptanalytical attack can only be achieved if (a) the volume of traffic carried by a particular edition of this type of table is rigidly controlled and restricted, (b) a really sound disguised starting point indicator system is used, and (c) the Basic Book is not compromised physically or through overuse. (One-time Pads are of course excluded from this reasoning).

7. By the beginning of 1942, it had become apparent that the traffic carried by the General (M) Table was rising so rapidly that drastic steps would be required to control "depth" as far as practicable. Twofold action was taken. Firstly, the rate of production and change of editions of the M Table was greatly accelerated; secondly, a third series of Tables (S.P.02436 - "S" Table) was prepared for exclusive use in the North Atlantic and Home Waters. As an emergency measure, pending production and distribution of this new "S" Table, two editions of a standard British recoding table (S.P.02361 series) were set aside and used for the purpose. The first of these was made effective on the 1st April, 1942. Of necessity, however, owing to shortage of "follow-up" editions it had to be retained in force for three months (i.e. until the 1st July, 1942). Although this resulted in a very

heavy "depth" (see Chart), it nevertheless served a useful purpose in diverting a large volume of traffic off the more heavily used general (M) Table. From the 1st April, 1942, the British-U.S. Tables conformed to the new British Double Indicator System; i.e. four-figure family of Starting-point Indicators common to all Tables. The second specially allocated British Table was made effective on the 1st July, 1942, and was replaced on the 1st August by the first of the new (S.P.02436) Tables.

8. Meanwhile, the rate of production of both the General (M) and North Atlantic (S) Tables was still further accelerated to the maximum possible. The following statement shows rates of change of both series from the 1st July, 1942, to 31st December, 1943:

"M" Table.	1st July to 1st Sept., 1942	Monthly editions.
	1st Sept., 1942 to 1st Feb., 1943	15 day editions
	1st Feb., 1943 to 31st Dec., 1943	10 day editions
"S" Table.	1st July to 1st Nov., 1942	Monthly editions.
	1st Nov., 1942 to 1st Feb. 1943	15 day editions.
	1st Feb., 1943 to 1st Dec., 1943	10 day editions
	December, 1943.	8 day editions.

9. This progressively increased rate of change was the best that could be achieved having regard to production and (more particularly) distribution problems inherent in such an accelerated programme. That it by no means solved the problem of excessive loads on the tables was appreciated at the time, and is illustrated in the accompanying Chart.

10. In an endeavour to divert a proportion of traffic off these heavily used tables, Navy Department was, in June 1942, supplied with the current editions of British Naval Cpher and Naval Code with their associated general and Area One Tables. In August, 1942, distribution of these S.Ps. was for a like purpose extended to the Commanders of American Sea Frontiers. Naval Code and Commander-in-Chief Western Approaches Code "OUT" Pads were also issued to certain U.S. warships whilst working under the operational control of Commander-in-Chief Western Approaches.

11. Traffic in the "M" and "S" Tables continued, however, to rise sharply, and in August 1942 peak depths were reached on both tables; this was accounted for only in part because the August traffic was the

the highest yet reached; the major contributory cause was introduction of the "Left and Right procedure" for both Tables on the 1st August, 1942, thus virtually halving the number of groups available in each table for recyphering the subject matter of signals.

12. From the 1st September, 1942, the "M" Table changed every fifteen days, and from the 1st February, 1943, every ten days. Similar accelerations in the rate change of the S Tables were effective on the 1st November, 1942 and the 1st February, 1943. The falls in depth consequent upon these accelerated changes are shown on the Chart.

13. This disguised indicator procedure was for the first time made effective on the 15th December, 1942, for all three British-U.S. Tables. The effects of our various alterations in Indicator Procedure are discussed elsewhere in this review.

14. By April, 1943, Naval Cypher No. 3 had been in force, for practical purposes, some eighteen months. It had long been appreciated that a change of edition was much overdue, since it had to be assumed that, although not physically compromised, the recyphering tables had been so heavily used that recovery by the enemy of many groups from the basic book was certain. It was not practicable to set aside another edition of Naval Cypher specially for British-U.S. use; the fact that No. 3 was so used had already reacted unfavourably on us to the extent that we had been obliged to retain the standard British editions in force far longer than was anticipated. Thus Naval Cypher No. 2 had necessarily to remain in force from the 20th August, 1940, until the 1st January, 1942, and, in April 1943, Naval Cypher No. 4 had been in force since the 1st January, 1942. It had already been planned to make Naval Cypher No. 5 effective for British use on the 1st June, 1943, and by agreement with the Navy Department it was later decided that No. 5 should also replace No. 3 on the same date, and that thereafter there would be one common Naval Cypher both for R.N. and for British-U.S. communications. In point of fact, Naval Cypher No. 5 was made effective for British use on the 1st June, 1943, as planned, but

TOP SECRET

owing to a last minute delay in American distribution, was not made effective for combined use, in place of No. 3, until ten days later; 10th June, 1943. Meanwhile, as a safety precaution pending introduction of the new Cypher, all the groups in the Position and Compass table of Naval Cypher No. 3 were cancelled on the 10th April, 1943, and new ones allocated. This measure was taken since analysis showed that the Position and Compass Table groups, which were of course vitally important ones, had been used excessively. At the same time, a general warning was issued to all holders of Naval Cypher No. 3 that these new groups must be used for cyphering positions and that for this purpose use must not be made of the already heavily used groups from the Numbers Section of that book.

15. In May 1943, a further endeavour was made to relieve the pressure on the "M" and "S" Tables. This took the form of requesting the Navy Department to accept use of the standard British Naval Cypher and Naval Code, with associated Tables and One-Time Pads, in all American warships co-operating with us in North Atlantic Escort work. The Navy Department would not agree, however, and the proposal had reluctantly to be dropped.

16. As stated in paragraph 14, Naval Cypher No. 5 replaced No. 3 on the 10th June, 1943. No. 5 and subsequent editions of Naval Cypher incorporated certain security improvements, such as alternative groups for common words and phrases and the abandonment of self-evident "switch" groups. This edition remained in force until the 31st December, 1943, when it was replaced by No. 6., and the Stencil Subtractor system.

17. This was followed on the 1st July, 1943, by the use of Lettered Co-ordinates (S.P.02274) for expressing positions in the daily U-Boat situation reports. This additional security measure co-incided with the improved security of the Tables of Lettered Co-ordinates, which was provided by a fortnightly, instead of monthly, change of Table as from the 1st July, 1943.

18. Meanwhile, the Navy Department had been experimenting since early 1942 with a Combined Cypher Machine to replace Naval Cypher as

a combined system, and on the 1st November, 1943, machines had been sufficiently distributed to enable the system to be made effective in the North Atlantic, thus providing a welcome relief for the "M" and "S" Recyphering Tables. It was many months, however, before the system was sufficiently widely held to be of substantial value in easing the load on the Tables.

19. Call Signs. It was quite impracticable, in 1941, for the standard R.N. system of Call Signs and Delivery Groups to be extended to provide also for British-U.S. communications. Concurrently therefore with production of the British-U.S. recyphering tables referred to in paragraph 3, successive editions were put in hand here of a special book of British-U.S. Call Signs (S.P.02378 series). The first of these editions was made effective on the 16th June, 1941, concurrently with the first "M" and "H" Tables. Three successive editions followed during the period under review, i.e. up till 31st December, 1943. These call signs had necessarily to be used both as such and as Delivery Groups, and since (a) they were not, and could not satisfactorily be, subject to any recoding process, (b) their composition was necessarily such as to make them self-evident as British-U.S. call signs, and (c) each edition had to be retained in force for many months, their security value was extremely low. This factor is a further one which militated against the security of the British-U.S. recyphering tables, since the enemy could:-

(a) Immediately recognise and segregate all four-figure W/T traffic using the British-U.S. call signs, and concentrate on it with the certain knowledge that British-U.S. recyphering tables had been used

and

(b) By breaking down the significations of call signs, greatly profit in his endeavours to recover groups from the basic book and from the recyphering tables. (Note: Introduction of the Left and Right procedure on the 1st August, 1942, tended to confine recoveries to the left hand pages of the table).

20. This state of affairs was, of course, appreciated at the time, but no remedial action was possible, short of the various palliatives enumerated earlier in this section. In 1943, however, after prolonged discussions with the Navy Department, work was

TOP SECRET

put in hand of an entirely new and secure system of British-U.S. call signs and delivery groups, modelled on the lines of our own forthcoming new system. Due, however, to a number of technical difficulties, and certain misunderstandings by the Navy Department, it was not possible to make this new system effective until the 1st July, 1944, four months after the new system had been made effective within the Royal Navy. Although the new system provided secure call signs and delivery groups, it was still impossible to overcome the drawback by which British-U.S. call signs and delivery groups remained distinctive as such.

21. Summarised, therefore, it can be stated that from the date America entered the war on the 7th December, 1941, until the 31st December, 1943, after which the new and much more secure Stencil Subtractor recyphering procedure was effective, we were compelled to fight an up-hill battle for security in the face of unavoidable difficulties in the way of huge traffic loads, far in excess of the carrying capacity of the Long Subtractor Tables, and an unsatisfactory call sign system which assisted the enemy in his attacks on the British-U.S. re-cyphering tables.

TOP SECRET

PART I - SECTION B - LOW - GRADE SYSTEMS.

FLEET CODE. The first edition of Fleet Code in its present form was brought into force on the 1st May, 1936, when it replaced the old four-letter Peace Code which had been effective since 1923.

2. On the outbreak of War, Edition No. 2 was in force and remained effective until replaced on the 20th January, 1940. Editions were subsequently replaced at irregular intervals in accordance with the policy of bringing a new edition into force prior to an important operation and changing it after the operation. Up till November, 1943 the average life of editions was approximately two months.

3. On the 16th June, 1941, concurrently with the date Naval Cypher No. 3 was made effective for British-U.S. use, Edition No. 13 of the Fleet Code was brought into force exclusively for British-U.S. communications. Edition No. 13 remained in use for this purpose until replaced on the 1st November, 1942, from which date normal British editions were used both for intra R.N. and Limited Combined signalling.

4. Special editions of Fleet Code were set aside from time to time for combined and limited combined use during major amphibious operations, such as "TORCH" and "HUSKY". For operation "OVERLORD", the normal editions were used but prior to, during and for a month after the assault, the rate of change of editions was accelerated to fifteen days.

5. Resulting from experience in "TORCH" and "HUSKY", the design of Fleet Code was changed to incorporate numerous words and phrases in common British and U.S. five-services use in connection wit amphibious such combined/operations, and the code was renamed the "Fleet and Combined Operations Code." The first of these new ditions became effective on the 30th June, 1944.

6. Since the Americans had nothing comparable to Fleet Code in the way of quick and reliable battle code, the book proved invaluable for limited combined Naval use in the Atlantic and the Mediterranean.

TOP SECRE

7. When, however, the British Pacific Fleet adopted American communications systems, in February, 1945, the Fleet Code was withdrawn from all units of the B.P.F. and from U.S. warships in the Pacific. For tactical signalling use was made instead of the U.S. Aircraft Code (Pacific Edition).

SMALL SHIPS CODES.

8. The problem of devising a small-craft code with reasonable short-term security has always been a difficult one, and hitherto it has not been satisfactorily solved.

9. For the first two years of the war Syko (with Naval Cards) was used as the standard low-grade system for communication with vessels such as Auxiliary Minesweepers and anti-submarine craft, Examination Vessels, Harbour Defence and Local Craft, M.T.Bs., M.Ls., etc., none of which of course carry a high-grade system. Syko was obviously, however, unsuitable in many respects; its security was very low and the method of coding was both tedious and slow.

10. A Small Ships Signal Code was therefore designed following experiments as to the most suitable type of book for use in small craft. This Code included a short vocabulary with words and phrases most commonly used in small craft. Each work or phrase was allocated a two-letter group and (in the interests of simplicity and rapid handling) these groups and their significations were arranged in alphabetical sequence thus precluding the necessity for a separate code and decode. Separate daily codes (pages) were provided for use during every twenty-four hours. The daily codes changed at midnight. The first of these codes (S.P.02383) was brought into force at Home in August 1941. The prefix "LOXO" was used to indicate use of the code. This type of code continued to be used both at home and abroad until the 1st December, 1942, when, in an endeavour to achieve greater security, two editions of the code were made effective concurrently on the Home Station. Even-numbered editions were used exclusively by Harbour Craft, Inshore patrols, Auxiliary Minesweepers and other small craft on passage from port to port, etc., whilst the odd-numbered editions were reserved for use by M.T.Bs., M.G.Bs., M.Ls., and other small craft employed on active operations, coastal convoy duties. Even and odd numbered editions were distinguished as such

by the prefixes LOXEN and LOXOD respectively.

12. In 1943, this code was replaced by four separate series of Small Ships Codes. On the 1st August, 1943, S.P.2538 Small Ships Signal Code (LOXO) was brought into force at Home. This comprised words and phrases to which were allocated three-letter groups arranged in sequence as was the case with the earlier codes described above. Each monthly edition comprised thirty-one pages of separate codes - one for use on each day. This code was provided for use by small craft engaged on local, as opposed to operational, duties. The daily codes changed at midnight.

13. This was followed on the 1st September, 1943, by S.P.2534 (COFOX) a Small Ships Operational Code for use by M.T.Bs., M.G.Bs., etc., engaged on active operations. In this code, the groups were hatted two-letter ones and each monthly edition comprised thirty-one daily changing codes and decodes. The daily codes changed at noon instead of midnight (as was the case with the Signal Code) for convenience of craft engaged in night operations. Two similar series for use abroad (FOXO and MEDOX) were made effective in the Mediterranean in July, 1943, and extended later to other areas.

14. Between the 1st April, 1944, and the 1st October, 1944, these codes were replaced by a Small Ships Basic Code having numbered groups which were converted into three-letter Groups by means of daily changing coding cards. The new type LOXO code was effective at home on the 1st April, 1944, and the COFOX code was effective at home on the 1st October, 1944. The new type MEDOX and FOXO codes became effective abroad on thelst September, 1944, and the 1st October, 1944, respectively. The times of change of the daily Cards remained as before; i.e., the Signal Code Cards changed at midnight and the operation Code Cards at noon. This system of a non-confidential basic figure code used with daily changing Coding Cards remained effective until the end of hostilities. The Security afforded by these daily changing Coding Cards was, of course, known to be very low, and warnings were repeatedly issued that it must be appreciated the enemy would probably read messages made in them after a time lag varying from upwards of a few hours only, depending on the volume

TOP SECRET

of traffic. There was, unfortunately, however, no alternative system available and these security disadvantages had necessarily to be accepted.

15. From the practical handling point of view the codes were excellent. LOXO was used extensively throughout operation "OVERLORD" as a low grade British Naval and Limited Combined British-U.S. system. Recommendations with regard to the future policy for Small Ships Codes will be found in Part III, Section B of this Review.

OTHER LOW-GRADE SYSTEMS, AUTHENTICATION TABLES, ETC.

16. Syko, Cysquare, Aircraft Reporting Code, Etc. The Syko system was first made effective in the Navy early in 1939, when general distribution was made of the device together with Naval Peace Cards for use with it.

17. On, and immediately after, outbreak of hostilities, Naval War Syko Cards (NYKO S.P.02255 series) and R.A.F. War card (S.P.02266 series) were brought into force; these were followed early in 1940 by Inter-service Syko Cards (S.P.02342 series).

18. In March 1942, "Rekoh" cases were issued for use with Syko Cards, to take the place of Syko devices which were in short supply. In the same month a special series of R.A.F. Middle-East cards (S.P.02433 series) was made effective for Naval and R.A.F. use in the Mediterranean Area.

19. As a measure of security, it was decided to introduce a special series of Syko cards for use exclusively in the North Atlantic, for communications with shore-based aircraft operating from the United Kingdom and Gibraltar, and on the 1st April, 1942, this special series was made effective. Use of these cards had necessarily to be distinguished by the self-evident prefix: COCO.

20. On the 1st June, 1942, use of the Inter-service Syko cards ceased at home and were replaced by an entirely novel letter-for-letter transposition system known as "cysquare".

21. The security of Syko had long been known to be extremely low, and was the subject of much investigation. Various methods of increasing its security were examined but discarded as unsatisfactory. The only practical solution which would afford some small added security was to introduce non-reciprocal cards; these were first made effective on the 1st July, 1942.

22. The Cysquare system referred to in para. 20 proved unsatisfactory, both from the security and practical handling points of view. It was therefore discontinued on the 1st March, 1943, from which date there was made effective at home an Inter-service three-figure code (cypher) using four-figure long-subtractor tables, with four-figure Starting-point Indicators sent plain. Messages in this code were distinguished by the self-evident prefix "ROOM". This code was later withdrawn (on the 1st January, 1944).

23. On the 1st May, 1943, use of the Inter-service Stencil cypher was abandoned, ~~and~~ since the advent of Inter-service cypher had made the former system redundant.

24. On the 1st June, 1943, the R.A.F. World-wide War Syko Cards (S.P.02308 series) replaced the old type R.A.F. General series of cards (S.P.02266).

25. It had long since become evident that a more secure system than Syko was desirable for communication with shore-based aircraft operating from the United Kingdom and Gibraltar, since provision of the special COCO cards referred to in para. 19 was by no means the most satisfactory answer. An Aircraft Reporting Code (S.P.2488) had therefore been compiled and was made effective on the 1st July, 1943, to replace the Coastal Command Syko Cards. This code proved extremely satisfactory and gave greatly increased security in the form of daily changing codes and decodes with words and phrases to which were allocated three-letter hatted groups.

26. In November, 1943, "Rekoh" cards were used first time, to replace Syko Cards and the "Rekoh" cases referred to in para. 18.

27. As stated earlier, Fleet Code had proved its usefulness as a Combined Code for use in amphibious operations, and it was decided by the C.C.B. Washington to produce a special code for use on such occasions, modelled on the general lines of Fleet code but having a specially adapted vocabulary. This resulted in production of the Combined Assault Code. Four separate series were produced; one for use in each of four separate Areas. The Code was a three-letter hatted one used with self-evident four-letter descriminators to distinguish it from Fleet Code. It was first used in June 1944 for Operation "OVERLORD", and proved highly successful.

TOP SECRET

28. Authentication Tables. In order to meet the American desire for authentication of signals, Combined Authentication Tables were produced by C.C.B. Washington and were first made effective for operation "OVERLORD" in June, 1944. Little, if any, use was in fact made of them, certainly by the Royal Navy, and whatever useful purpose they might have served was largely defeated by a succession of compromises. They were withdrawn from use at Home after the defeat of Germany.

TOP SECRET

PART I - SECTION C.

MERCHANT SHIPS' COMMUNICATIONS.

From the beginning of the war up till the 11th January, 1940, the only code for use with merchant ships was the International Code and a Naval Appendix to it (O.U.5500), recoded by means of a General Recoding Table, using bigram reciprocal substitution (S.P.02183series).

2. Call Signs were provided from the first edition of S.P.02182, ("Mercantile Secret Call Signs") which became effective on the outbreak of hostilities.

3. A Merchant Navy Code with four-letter hatted groups (S.P.2310) had, however, been prepared in anticipation of war, and was in course of distribution when hostilities broke out. This code, together with the first edition of a series of general recoding tables (S.P.02272) for use with it, was made effective on the 11th January, 1940, to replace the International Code, Appendix and Tables referred to in para. 1. The general tables for use with Merchant Navy Code were also at first bigram reciprocal substitution ones. There was no regular rate of change for these tables at this period, nor in fact could such a programme have been introduced, since editions were constantly in a state of compromise, and the best that could be done was to issue warnings regarding their insecurity and change editions as fast as new ones could be produced and distributed. Thus, throughout 1940, and indeed throughout the War, the average life of an edition was approximately two months, but editions known or suspected to be compromised physically had nevertheless to remain in force till new editions were ready. These simple substitution Tables was replaced in October, 1941, by Multiple-Alphabet ones (see later). Two editions of the General Table were in force concurrently throughout the War.

4. On the 10th October, 1940, as an additional security measure, a new series of "Commodores Recoding Tables" (S.P.02335) was made effective. These tables were multiple-alphabet ones with 30 pages, each of 15 alphabets. They were provided for use only when a convoy was unescorted or when the convoy had become detached from its escort

TOP SECRET

and it was essential to pass a message to the Commodore of Convoy by W/T. In practice, very little use was made of this series, and up till the 1st June, 1943, when it was finally withdrawn, six editions only were used; thus each edition was effective on an average for rather over five months.

5. Meanwhile, it had become clear that some more secure medium that the general tables was essential for communication with unescorted merchant ships. To provide for this, a series of "Independent Ship" (INDSHIP) tables had been prepared, and the first edition was made effective on the 30th May, 1941. The table was a multiple-alphabet one containing 50 pages, each of 15 alphabets, and included 1,650 four-letter indicating and check groups. The first edition was used for communication with independently routed British Ocean-going Merchant Vessels of less than 15 knots. Use of edition No. 1 was extended on the 22nd August, 1941, to ships over 15 knots, pending introduction of a special system of "one ship pads" for such ships (see para. 8 below).

6. In order to improve the security of communications with Merchant Ships in Convoy, a new series of Tables was made effective on the 1st June, 1941. At this stage, these tables were termed "Shipcon" tables (S.P.2388) (later OUTCON Tables). A new edition was, from that date, issued and used for each outwardbound convoy from the United Kingdom to North America. These tables were small multiple-alphabet ones containing only four pages of 15 alphabets each, together with twenty four-letter indicating and check groups.

7. From the same date (1st June, 1941) a new edition of the Mercantile Secret Call Signs was made effective (S.P.02182(2)).

8. In June 1941, a scheme was prepared to provide one-time pad communication with all fast independently-routed merchant ships. A thousand five-figure group pads each with 3,000 groups (S.P.2413 One Ship pads) were produced with the intention that one each should be issued to each Merchant Vessel for use, firstly, with a special five-figure "Diversion Code" (S.P.0242), and later, with the new Merchant Ship Code which would replace the existing Merchant Navy Code and would have five-figure groups in addition to four-letter ones. In practice, however, the intention to use these pads for one time signalling was found impracticable owing to the impossibility of

TOP SECRET

controlling the use of starting points by numerous originators all using the same pad. They were therefore used as normal long subtractor Tables.

9. On the 22nd August, 1941, these Oneship pads, together with the five-figure diversion code referred to, were ordered to be brought into force on receipt, for communication with all independently-routed ships 15 knots and over, and certain independently routed Oceangoing Tankers in the Atlantic.

10. The Diversion Code used with these pads contained 1050 five-figure groups allocated to a short vocabulary and to Numbers, Position and Compass Tables. For the reason stated in para. 8, the pads could not be used as one-time ones. Self evident Starting-point Indicators were used, and the number of the pad was expressed in Plain Language. Diversion Code and the first oneship pad were, in fact, issued on the 10th September, 1941. Use of Diversion Code with these pads ceased upon introduction of Merchant Ships Signal Book Volume II on the 15th April, 1942.

11. In September 1941, the "Ship Con" series referred to in para. 6 was extended to provide similar tables for inward-bound convoys (S.P.2406 - known as "INCON" Tables). These tables were four-page multiple-alphabet ones identical to those described in para. 6 for outward-bound convoys. (OUTCON tables).

12. On the 3rd October, 1941, the General (S.P.02272) Tables became Multiple-Alphabet ones of the same size as INDSHIP [illegible] Tables (50 pages, each of 15 alphabets).

13. Meanwhile, the first edition of the INDSHIP table, which from the 22nd August, 1941, had been effective for Independently routed ships both over and under 15 knots, was withdrawn on the 2nd October, 1941 from the fast ships, who were issued instead with a separate edition (No. 2); Independently routed Tankers in the Atlantic likewise used this edition. This was followed on the 9th February, 1942, by edition 3 of the INDSHIP series being made effective (concurrently with edition 1) for use by British oceangoing merchant ships of less than 15 knots. At this period, therefore, two separate series of the INDSHIP Tables were effective; one (editions No. 1 and 3) for ships

TOP SECRET

under 15 knots and one (edition 2) for ships over 15 knots and Tankers.

14. On the 15th April, 1942, it was possible to start use of the new Merchant Ships Signal Book (Mersigs Volume II). Until distribution of the new book was completed, however, it had to be used concurrently with the old Merchant Navy Code, and therefore, as a temporary measure, signals in the new book had to be distinguished by the plain-language prefix "Mersigs". An undesirable state of affairs from the security standpoint, but inevitable. The new book still retained the four-letter groups, but incorporated five-figure ones also since it had been decided that in the interests of security all Merchant ships tables should be converted into subtractor ones as soon as possible.

15. On the 29th April, 1942, edition (1) of the INBSHIP series was withdrawn from use. The position then remained that edition (3) was used by ships under 15 knots, whilst edition (2) remained effective for the over 15 knots and the Tankers.

16. Resulting from a general review of the security afforded by the INCON, OUTCON and Oneship pads, it was decided, and promulgated on the 4th May, 1942, that it was not compulsory to use secret reference positions in signals recoded by means of these series; i.e. that positions expressed in latitude and longitude or bearing from a known geographical position could be used. Except for a break from the 3rd December, 1943 to the 6th September, 1944, this procedure remained effective until the end of hostilities for the Incon and Outcon Tables, but it was considered advisable on the first date mentioned to re-introduce and retain permanently the precautions of lettered positions for signals recoded by oneship pads.

17. Distribution of the Oneship pad series was extended in July 1942 to all British and Allied ocean-going ships of 15 knots and over and to all British and Allied tankers irrespective of whether in convoy or independently routed. On the 22nd July, 1942, edition (4) of the Indship tables replaced editions (2) and (3). From then until the end of hostilities, the policy became that the Indship tables were issued only to independently routed ships under 15 knots other than

TOP SECRET

tankers, i.e., independently routed ships not holding Oneship pads.

18. Resulting from a further review of the security of the Oneship pads, certain changes in the procedure for use of these pads were made on the 15th November, 1942. It was emphasised that originators must select starting points haphazard and must discontinue the practice of "working through" their pads, since this, of course, imposed undue wear on the earlier portions of all pads; secondly, the practice of indicating the pad number was discontinued, since this was of some assistance to the enemy and was moreover unnecessary since the ship itself had of course only the one pad, whilst other authorities concerned were aware of the pad held by each ship and could, therefore, determine the number of the pad used from the secret call sign of the ship addressed. This was followed up, on the 15th December, 1942, by a further warning of the importance of selecting haphazard starting points and, since many originators had made a practice of starting on the first page, it was ordered that no messages should start on that page. This practice remained effective until the end of hostilities.

19. It had become apparent in 1942 that the security of the Mercantile Secret Call Signs in S.P.02182 series was frequently prejudiced by improper use of the call signs by merchant ships, and from the 6th January, 1943, there was made effective a system of Mercantile General Call Signs similar to the Naval General Call Sign system. Thereafter, merchant ships originating a message in code used a general call sign (NUMS 1 to 9) and disclosed her identity by coding up her secret call sign as the first groups of the message.

20. On the 15th February, 1943, S.P.02182(4) was brought into force to replace (2) which had been in force since the 1st June, 1941. No. (3) had been compromised and was not used.

21. Meanwhile, Outcon and Incon tables had been produced as subtractor ones for use with the new Merchant Ships' Code. The first of these subtractor tables were very small ones, comprising one page only with 150 groups, and thirty four-letter indicating and check groups. The first Outcon Subtractor table was issued on the 18th January, 1943, and the first Incon subtractor table, on the 8th April, 1943.

TOP SECRET

Use of the old type short multiple-alphabet tables ceased on the 15th March, 1943, for Outcons, and on the 24th August, 1943, for Incons.

22. On the 26th March, 1943, it was decided to extend the issue of Oneship pads to Neutral ships, 15 knots and over, trading in the Allied interests.

23. By the 20th May, 1943, it was possible to make effective the first of the Inship long-subtractor tables to replace the old type multiple-alphabet ones. The new tables comprised 50 pages, each of 150 groups (i.e., 7,500 groups), and each was provided with a liberal allowance of indicators (1650 four-letter indicator and check groups). This was followed on the 20th July, 1943 by edition 26 of the General table (S.P.02272) which was the first of a similar type of general long-subtractor tables.

24. Scrutiny of the volume and nature of traffic in the new type subtractor Outcon and Incon tables showed that 150 groups (which was all each edition contained) was insufficient for security. Use of these tables, of course, was evident to the enemy, and with 150 groups only it was apparent that he was being presented with dangerous depths, even during the very short life of each edition. Production was at once therefore put in hand (in October 1943) of larger tables with five pages of 150 groups each (i.e. 750 groups), 30 four-letter indicator and check groups continued to be provided.

25. In 1943, further investigations and analysis of merchant ships traffic disclosed the fact that it was undesirable to exclude the current type Incon and Outcon tables (or even the Oneship pads) from the rules necessitating use of secret reference position-s; on the 3rd December, 1943, therefore, use of secret reference positions was again made obligatory in <u>all</u> messages recoded by Merchant Ships tables and pads.

26. The security of individual oneship pads had always been an uncertain factor, since there was no ready means of ascertaining precisely to what extent a particular pad had been used. In December, 1943, a general replacement programme for oneship pads was therefore started. Pads were replaced in chronological order of their dates of original issue to ships.

TOP SECRET

27. In April and May 1944, the first of the new type of enlarged Incon and Outcon tables came into use. The first large Incon table was made effective on the 13th April, 1944, and the first Outcon on the 21st May, 1944. Instructions were issued that these large (five-page) editions were invariably to be issued, if available, in preference to the old one-page tables; the latter continued, however, to be issued to Convoys for some time further.

28. With the introduction of edition (13) of the Indship tables on the 20th April, 1944, an automatic monthly change of editions of this series was introduced;; this represented a very considerable advance on the period of two to three months which editions had hitherto had to remain in force until sufficient reserves had been built up. This monthly changing programme held good until Inship tables were withdrawn from use after cessation of hostilities with GERMANY.

29. The U.S. Navy Department had meanwhile suggested production of special convoy tables for use by American East Coast Convoys. These were prepared by the Government Code and Cypher School and consisted of ten-page subtractor tables. They were first made effective on the 29th July, 1944.

30. Urgent consideration had meanwhile been given to what steps could be taken still further to improve security of communications with merchant ships in convoy. The enlarged subtractor tables had been effective since April and May 1944 (see para. 27 above), but as a further measure of security it had been decided to incorporate in each edition of these tables a separate small Diversion Code; i.e., a new set of basic groups were provided with each recoding table. This, of course, represented a great advance in security, since it enabled the recoding process to be applied to groups other than the standard ones in Mersigs Volume II, all of which had necessarily to be considered compromised either physically or by reason of excessive use with low security tables. This new type of Incon and Outcon tables became effective for all convoys sailing after the 1st September, 1944; and from that date there can be little doubt that

TOP SECRET

this system of communication with convoys was secure. From the 6th September, 1944, onwards, therefore, it was once again permitted, when using Incon and Outcon tables, to express positions other than by means of reference to secret lettered positions.

31. A new edition of the Mercantile Secret Call Signs (S.P.02182(5)) was brought into force on the 1st September, 1944, to replace edition 4 which had been effective since the 15th February, 1943.

32. In order to provide additional security for communications with Merchant ships of the British Pacific Fleet Train, three unused editions of the Indship series were allocated to Rear Admiral, Fleet Train, on the 17th March, 1945, for use as such exclusively, and a special series of Pacship tables for this traffic was put in hand.

33. Issues of Incon and Outcon tables ceased after Convoy UC 71 sailed on the 3rd June, 1945, a month after termination of European hostilities. In the same month, use of the Indship series ceased in the non-combat Area, and ceased world-wide in July 1945 following an arrangement which was made effective for a separate series of editions of the general table (S.P.02272) to be used exclusively within the combat area. Use of Oneship pads also ceased in June 1945 in the noncombat area, except for signals to troopships. The programme of replacements of pads of this series was also discontinued. Control of the oneship pad series was vested in the U.S. Navy Department from the 1st August, 1945, onwards.

TOP SECRET

PART II - ENEMY CRYPTANALYTICAL SUCCESSES.

P R E F A C E.

Part II of this review aims at placing on record for the Naval Staff, a clear-cut and reasonably short account of the successes andfailures of Naval Cryptographic Systems in the face of systematic enemy cryptanalytical attacks. So far as practicable, the record is written chronologically, starting from the period immediately preceding hositilities on the 3rd September, 1939 and continuing until the end of the War with GERMANY in May, 1945.

2. No attempt has been made to incorporate a detailed history of the highly technical methods by which the Germans succeeded in reading some of our systems, nor of the enemy's widespread and intricate cryptanalytic and Traffic Analysis Organisation for doing so. Such a matter is outside the general scope of this review, and is moreover available in extenso from a great quantity of captured enemy documents and from records of interrogations of personnel of the German Cryptographic Organisation which were conducted by G.C.C.S. and Admiralty Technical Officers in the period immediately following cessation of hostilities. All information obtained from these sources has been sifted, evaluated, and recorded by the G.C.C.S. in co-operation with Admiralty, and copies of the resulting reports issued are held by the Naval Staff. It is, however, from these sources that Part II of this review has been compiled.

TOP SECRET

PART II - ENEMY CRYPTANALYTICAL SUCCESSES.

SECTION A (I) - HIGH-GRADE BOOK SYSTEMS.

BOOK SYSTEMS.

Naval Cypher - the Germans first broke into our long subtractor system early in the summer of 1938. This they did through the "Secret" Recyphering Tables for use with Administrative Code which were then brought into force for the first time. Their work was greatly facilitated by reason of the fact that the Administrative Code itself had been in use, unrecoded, since 1934, and hence they had succeeded by 1938 in largely reconstructing that book. At first, they had insufficient staff to deal also with Naval Cypher, but a few months later they had progressed so favourably with breaking Administrative Code that they were able to start entry also into Naval Cypher. Work on the latter progressed on a limited scale until a set-back occurred on the 25th August, 1939, when we changed editions of the General, Commander-in-Chief and Flag Officers' Recyphering Tables. By about the middle of October, 1939, however, they had again succeeded in breaking into Naval Cypher to the extent of reading a small proportion of messages. No attempt was made by the Germans to break all messages intercepted; work was rather concentrated on traffic in the North Sea and the Skaggerak, etc. When the German heavy-units made their first sortie at the time of the sinking of H.M.S. RAWALPINDI, the enemy read a number of cypher messages concerning counter measures taken by us. Entry into Naval Cypher through the Submarines Tables was facilitated because, at that time, Submarines used the General Recyphering Tables which were in current use for the great bulk of all Cypher traffic.

Note: It was not until May 1940 that a special table was set aside for Submarines and vessels operating in dangerous waters, and not until the 20th August, 1940, that Submarines ceased to carry Naval Cypher altogether and used instead Naval Code with recoding tables held exclusively by Submarines.

2. By the Spring of 1940, his work on Naval Cypher had so progressed that the enemy were able to read virtually everything of importance in connection with the Norway Operations. At this period some 30% to 50% of intercepted cypher traffic was read.

TOP SECRET

3. This state of affairs continued until the 20th August, 1940, when the old Naval Cypher (which had been current since 1934) was replaced by Naval Cypher No. 2. This change co-incided with a change of the General Recyphering Table and introduction of Naval Code, traffic in which now became externally identical with Naval Cypher traffic and so hindered the enemy in his efforts to segregate one from the other. This resulted in a temporary setback to the enemy, but by the end of September 1940 he was again reading a small proportion of traffic in Naval Cypher.

4. A further setback occurred on the 1st October, 1940, from which date was introduced the "Left and Right" recyphering procedure and also two additional Recyphering Tables: one for use only in Area I (Home and North Atlantic) and one in Area 2 (Mediterranean, East Indies and South Atlantic). These measures severely curtailed the enemy's progress for a short while and resulted in his having considerably to increase his cryptanalytical staff; with the increased staff, however, better progress was soon made, although the previous degree of success was not attained.

5. A far more severe setback for the enemy occurred on the 20th January, 1941, with the introduction of disguised Starting-point Indicators. For some four weeks the enemy could read nothing. He could not determine whether in fact we had changed the edition of Naval Cypher. (We had not). After about four weeks, however, he again broke into Naval Cypher but on nothing approaching the old scale. It was clear to the enemy that he would require twice, or even three times, the number of trained personnel if he were to achieve a reasonable measure of success, and this increase in staff was not immediately forthcoming. The methods by which success could be achieved appeared clear enough to him, but in the absence of sufficient staff, and since at that time he was not in possession of Hollerith Tabulating Machinery, he was faced with acute difficulties. Even after the four weeks referred to he could read barely 10% of the volume of traffic which had been available to him before introduction of disguised Starting-point Indicators.

TOP SECRET

6. On the 1st September, 1941, disguised Starting-point Indicators were abandoned by us in favour of a standard "family" of four-figure Starting-point Indicators for all tables. The main problem now facing the enemy was that of determining which table was used for a particular message, and he could no longer set about this task by breaking-down the disguised Starting-point Indicator. Bearing certain factors in mind, however, such as the increased use of Area Tables, he was nevertheless often able to determine which series was used; this was done partly by the normal cryptanalytical process of searching for repeats and difference, and partly by establishing the Table used with a fair degree of probability, from the routing of the message. Whereas, previously, the enemy had to compare all messages with one another, he now had to compare only those having the same four-figure Starting-point Indicators. The new system was, in fact, a retrograde measure from our point of view and we now knew that it proved of considerable assistance to the enemy. It enabled him soon to read again nearly half as much as he had been doing at the peak of his success immediately before the 1st October, 1940 when the "Left and Right" procedure and Area tables were introduced. Later, results obtained by him were so good that he virtually reached the old standard achieved before the recyphering of Indicators. This state of affairs continued until the Basic Cypher (No.2) was replaced by Naval Cypher No. 4 on the 1st January, 1942.

7. Meanwhile, traffic in Naval Cypher No. 3, which had been set aside for British-U.S. use, started to make its appearance in appreciable volume towards the beginning of October, 1941, and thereafter increased progressively.

8. The enemy very quickly appreciated the ~~initial~~ vital importance of Naval Cypher No.3, which he styled the "Convoy Cypher", and, from late 1941 onwards, he concentrated most of his energy on attempts to break it. Traffic in the cypher was necessarily distinctive by reason of the special British-U.S. call signs, and also of the fact that the old system of plain five-figure Starting-point Indicators was initially used. This factor was, of course, of notable assistance to the enemy in his work of segregating all such traffic for special

TOP SECRET

analysis. He soon realised that the cypher was used almost exclusively for North Atlantic Convoy Escort traffic, and he was able to make inroads upon the recyphered subject matter largely through the address, which could often be guessed with reasonable accuracy and was moreover expressed in the relatively insecure British-U.S. Call Sign system then in force. (Note: The "Left and Right" recoding procedure was not made effective for this Cypher until the 1st August, 1942). His attacks on the cypher were helped further by the fact that, until the 1st April, 1942, virtually the whole traffic in Naval Cypher No. 3 had to be recyphered by means of the one and only General "(M)" Table then available.

9. By the middle of February, 1942, very substantial progress had been made by the enemy in reading messages made in Naval Cypher No. 3, and the Cypher itself had been reconstructed by him with astonishing rapidity. In February and March 1942, the enemy had achieved such a degree of success that he was reading, after the briefest of time lags, a great proportion of all signals in connection with Convoys, not only in the North Atlantic but in other Areas where the cypher was used. This state of affairs continued up to the 15th December, 1942, and the fact that on the 1st April, 1942, the indicator system changed and became identical with the standard British four-figure system, or that from that date we introduced an additional (Atlantic area) Table, caused him little or no difficulty.

10. Meanwhile (as stated in para. 6) the standard British Naval Cypher (No. 2) had been replaced by No. 4 on the 1st January, 1942. The enemy had little success with this cypher for some months, partly because he was by then devoting practically all his attention to what, from his point of view, was by far the most important work, i.e., solving messages in the British-U.S. Cypher (No. 3), and in Naval Code recoded by Auxiliary Vessels Tables, and partly because, by then, we had succeeded in changing tables much faster, and we were, moreover, making far larger use of One-time pads, particularly in the Home and North Atlantic. (Note: In December 1941 and January 1942, One-time cypher out pads from Admiralty, Commander-in-Chief Home Fleet and Commander-

TOP SECRET

in-Chief Western Approaches were made effective). In particular, the enemy was deprived of valuable material in the way of Western Approaches Daily Routine SITREPS which, during most of 1941, were recyphered in the Area 1 Table, but from the 21st January, 1942, onwards were recoded in Commander-in-Chief Western Approaches Code "OUT" One-time Pad. By March 1942, the enemy had achieved some small success in breaking into the new Naval Cypher No. 4, and by October 1942, he had reconstructed the book to a fair extent. In that, and the succeeding months, he read a small number of messages in this Cypher relating to Convoy movements in the Pacific, Indian Ocean and Red Sea. The extensive and growing use of One-time Pads, however, continued to be a great hinderance to him, and he never achieved results with this cypher comparable with his earlier successes. (Note: Enemy work on our high-grade book systems was considerably helped from about the middle of May, 1942, onwards by his use for the first time of HOLLERITH tabulating machinery).

12. Reverting again to the British-U.S. Cypher (No. 3). As stated in para. 9 the enemy had made good progress with this cypher from early in 1942 onwards, and was little concerned by the changed Indicator System and the additional (Atlantic area) Table both of which became effective on the 1st April, 1942. He likewise was not handicapped to any appreciable extent by the fact that the "Left and Right" procedure was made effective with Naval Cypher No. 3 on the 1st August, 1942. The recyphering tables used with Naval Cypher No. 3 were, between early 1942 and the 15th December 1942, broken into by the enemy so successfully that there were times during this period when he appears to have succeeded in reading as much as 80% of the entire volume of intercepted traffic. On the 15th December, 1942, however, the disguised Starting-point Indacator system was re-introduced for all tables, including those used with Naval Cypher No. 3. This was a setback to the enemy, who had already experienced much trouble with this system when it was first introduced on the 20th January, 1941. By now, however, he had the benefit of having already worked on Disguised Indicators for some eight months in 1941, and he knew better

TOP SECRET

how to set about the problem, which did not present insuperable difficulties but was again rather a matter for a substantial increase in his staff. It was not long, therefore, before he was again breaking into Naval Cypher No. 3; and by February 1943, having succeeded in obtaining and training the largely increased staff, he was well on the way to achieving his former degree of success. He was frequently able to read virtually all the convoy traffic that interested him in the North Atlantic so quickly that on occasions he had movement information ten to twenty hours in advance. In this he was assisted to some extent by routine signals from Western Approaches and Halifax; also by reading much traffic in Merchant Ships' Code, particularly messages recoded in the Convoy Tables (See section C). Information from this source which was of tactical value to U-Boats, was transmitted by W/T to the Senior Officers of the U-Boat Packs concerned. Possibly the most disturbing feature in this connection is that from early in February 1942 until the 10th June, 1943, (when Naval Cypher No. 3 ceased to be used) the enemy was nearly every day able to read the daily Admiralty U-Boat disposition signal, often as early as midnight on the day it was made. By this he could forecast the probable routes of convoys which would be followed in order to avoid U-Boat concentrations referred to in the disposition signals.

13. On the 1st June, 1943, Naval Cypher No. 5 replaced No. 4, and on the 10th June, 1943, the same Cypher (No. 5) replaced the British-U.S. Cypher No. 3. Naval Cypher No. 5 was the first of a new type of editions incorporating a number of security improvements (see part I-A). From then onwards the enemy had no further success with Naval Cypher. Even had he achieved results working on his old principles, it is likely that they would have been short-lived, since from the 1st July, 1943, onwards, long subtractor tables started to be replaced by the Stencil Subtractor System which it is known the enemy was unable to break successfully, although he displayed great ingenuity in reconstructing the basic principles of the new procedure..

14. The enemy ceased all work on Naval Cypher on the 31st January, 1945.

TOP SECRET

ADMINISTRATIVE CODE AND NAVAL CODE.

15. The Administrative Code was first brought into force in 1934, when it was used unrecoded for non-confidential messages. The enemy started work on it almost at once, and was very shortly in a position to read signals to a limited extent. A large volume of intercepted traffic was, however, available to him, and after about six months so many groups had been recovered that the code could be read with comparative ease. Starting in 1938, the code was used both plain for non-confidential messages and recoded for confidential ones; this enabled the enemy to break for the first time into our long subtractor systems. He was assisted in his work by the relative infrequency with which Tables were then changed, and, in particular, by the insecure Indicator system then in force: i.e., a standard unchanging book of five-figure Table Indicators to denote the Table used, and five-figure (plain) Starting-point Indicators incorporated inside each Table. The enemy devoted much attention to this work from 1938 onwards, and by the time War broke out he was reading recoded Administrative Code extensively.

16. Up till the 20th April, 1939, the Administrative Code was used with two General Tables, one for recyphering and one for recoding, but after that date the General Recoding Table only remained. A new edition of the latter was brought into force on the 25th August, 1939, but this did not hinder the enemy greatly, and by the middle of September 1939, he was again breaking into the traffic. Extensive information on British Naval mobilisation was obtained from this source; also much patrol craft traffic was read in Home waters and the North Atlantic. A copy of the Administrative Code was captured by the enemy at Bergen in May 1940 but this was not of much practical value to him, since he had already succeeded in building up most of the Code by cryptanalysis.

17. This state of affairs continued until the 20th August, 1940, when use of Administrative Code ceased for good and it was replaced by the new "Naval Code" with four-figure groups, thus making the external appearance of messages in that Code identical to those in Naval Cypher. This caused the enemy a setback and it was some time before he could determine whether, in fact, two separate basic books were being used or

TOP SECRET

one only. The fact that two books were being used soon became apparent to him, however, from cryptanalysis, and after about six weeks he had succeeded in breaking into Naval Code.

18. From this date onwards, Naval Code was used also for communication with Auxiliary Vessels, and since traffic recoded in the Auxiliary Vessels Table was distinctive by reason of the Minor War Vessels Call Signs used, the enemy was able to segregate it from the rest of the Naval Code traffic and to devote special efforts to breaking it. This he continued to do with varying, but on the whole marked, success until the 1st December 1943 when the stencil subtractor system was introduced for the Auxiliary vessels Tables. Apart, however, from the Auxiliary Vessels traffic he devoted considerable attention to breaking Naval Code recoded by the Area I (Home and North Atlantic) Table, which came into force for the first time on the 21st November, 1940. As a rule, however, he concentrated only on breaking the address portion of such messages in order to discover positions of major units. The enemy also worked to some extent on the general (World-wide) Recoding Table for Naval Code and achieved some success, notably with signals to and from the Commodores of R.N. Barracks dealing with personnel questions; From this traffic he succeeded in deducing the location of a number of units in Eastern Waters.

19. The "Left and Right" procedure was effective from the 1st October, 1940 (except for the Auxiliary Vessels tables) but this curtailed the enemy success for a short time only. He very soon appreciated what had been done, and his work was not basically affected although additional personnel was needed. The "Left and Right" procedure was not introduced for the Auxiliary Vessels Tables until a year leter (1st October, 1941).

20. Introduction of disguised Starting-point indicators, on the 20th January, 1941 had of course the same affect as was the case with Naval Cypher; i.e. the enemy's work was greatly hindered and his staff requirements more than doubled.

21. This was followed, on the 1st September, 1941, by the return to plain Starting-point Indicators which (as with Naval Cypher) greatly

TOP SECRET

facilitated the enemy's work.

22. Meanwhile a copy of Naval Code (No. 1) had been captured in May 1941 from H.M.S. YORK, sunk in Suda Bay, CRETE.. The book is stated to have been permeated with sulphuric acid, and it is not clear whether it was wholly or partly illegible.

23. On the 1st of January, 1942, Naval Code No. 2 was brought into force. The enemy soon broke into the new code, and after about ten days was able to read some short messages mostly of a routine nature. His success increased throughout 1942 until re-introduction of disguised Starting-point Indicators on the 15th December, 1942. In this connection the remarks under "Naval Cypher" are equally applicable to Naval Code; it was a temporary set-back only, and until the 1st March, 1943, when Naval Code No. 3 was brought into force, the enemy continued to read a high proportion of traffic recoded by the Auxiliary Vessels Tables. A copy of Naval Code No. 2 was captured by the enemy at Tobruch at the end of 1942.

24. Naval Code No. 3 was the first of an improved type of edition incorporating several security advantages (see Part I - A) and its introduction on the 1st March, 1943, caused a break in enemy success. Nevertheless, by August, 1943, he had again broken into the Auxiliary Vessels traffic and continued to do so with increasing success up to the 1st December, 1943. From the 1st March, 1943, onwards, however, due to inadequate staff the enemy did little, if any, work on other than the Auxiliary Tables.

25. On the 1st December, 1943, the Auxiliary Tables transferred to the Stencil subtractor system, and thereafter the enemy failed to make any further progress. The same situation applied to virtually all other Recoding Tables, which by the 1st, December, 1943, had transferred to the Stencil Subtractor type.

26. It was apparent to the enemy immediately after the 1st December, 1943, either that a new edition of Naval Code had been introduced, or that some entirely novel recoding system for the Auxiliary Vessels Tables had been brought into force on that date, since from then onwards he could not break into traffic which hitherto he had exploited so successfully. His first impression was that

TOP SECRET

Naval Code (No. 3), which has been effective only since the 1st March, 1943, must have been changed on the 1st December, 1943, and that we had adopted this measure as a result of treachery by Badoglio, since the preceding editions had remained in force very much longer and he could therefore see no other logical reason for changing No. 3 after a life of nine months only. This was of course not the case; it was a routine change. Later in the month, however, he arrived at the correct solution; i.e. that the Code had remained effective but that a new recoding system had been introduced (this, incidentally he also attributed - quite wrongly of course - to Italian treachery!). Having arrived at this correct conclusion, the enemy set about trying to discover the nature of the new system.

27. With this aim, he concentrated on all available Auxiliary Vessels Traffic for the month of December, 1943, which was the last effective month of Naval Code No. 3 and the first month of use of the Auxiliary Vessels Stencil Subtractor recoding table. In this work he displayed an astonishingly high degree of skill and ingenuity, and, in January 1944, he had succeeded in establishing the principles of the Stencil Subtractor single conversion indicator procedure which was at that time effective. This afforded him an entry into the nature of the system generally, and in the course of succeeding weeks he succeeded in reconstructing some individual back (December 1943) messages and, later on, whole days' traffic (from December 1943) almost completely.

28. It had become apparent to the enemy that new Key Recoding Pages were effective each day, and his recovery of figures from Key Pages indicated that the latter were used under a stencil having windows in a constant (or more or less constant) position. Reconstruction of the complete stencil was then for him only a matter of time. A staff of some 250 was employed by him exclusively on this work, and, later, synthetic messages were prepared and coded in Naval Code and recoded by means of the Stencil Subtractor system, in order to test, practice and encourage the staff in their ability to break traffic recoded by the new procedure.

TOP SECRET

29. The enemy satisfied himself that, given sufficient traffic, the Stencil Subtractor system could be broken into currently, but only if a captured basic book were available, or the basic book used was one which had been in force for a prolonged period (at least six months) and from which groups had been substantially recovered.

30. Although the enemy thus succeeded, during the course of January 1944 and succeeding months, in breaking the December 1943 traffic in the Auxiliary Vessels table, he was able to do so only by reason of the fact that he was working with an edition of Naval Code which was then in its last month of life and from which a substantial proportion of groups had been recovered. He could make no further progress with traffic recoded from the new edition of Naval Code which became effective on the 1st January, 1944.

31. It is abundantly clear that the Stencil Subtractor system is far more secure than the old long-subtractor method. In the opinion of the enemy cryptographers, however, it has certain disadvantages in relation to the latter. For example, the enemy proved to his satisfaction that, if the basic book is known, not only parts of messages, but virtually all messages recoded on the same key sheet, can be broken given a known depth of as little as two. He estimated, however, that the staff required to do so would be five times as large as that needed to achieve comparable results with the long subtractor system.

32. In a periodical "Progress Report", dated the 5th January, 1945, enemy cryptographers assessed that from 80 to 100 messages recoded by the Same Key Sheet would suffice to obtain a break-in, assuming possession of the basic book. In these circumstances, they believed a break-in would take from two to four days, but that it might be possible to cut down this period with further experience and adequate staff.

33. Although, from the practical aspect of traffic exploitation, the enemy did not profit from his reconstruction of the Stencil Subtractor system, he (rightly) regarded his success in doing so as a very fine achievement in cryptanalysis. In about May 1944, he succeeded in obtaining from the sunk Canadian Destroyer "ATHABASKAN"

TOP SECRET

a copy of A.F.O"S"10/44 describing fully the Stencil Subtractor system, and this confirmed the accuracy of his reconstruction work. It appears, moreover, that the enemy succeeded in persuading a Leading Telegraphist taken prisoner from H.M.C.S."ATHABASKAN", to give "quite a detailed description of the new recyphering system." From A.F.O. "S".10/44 he became aware of the forthcoming introduction (on the 1st May, 1944) of the double-conversion procedure for Stencil Subtractor indicators, and from a captured (undated) enemy document dealing with the "cryptanalytic approach to the double conversion of indicators on the British Naval Stencil Subtractor" it is clear that he devoted intensive study to this problem and appears to have evolved methods by which he considered the double conversion process could be broken down.

34. The Auxiliary Code. At the outbreak of War, this four-letter code had been in force since 1937, and had been used extensively both plain for non-confidential traffic and (for confidential traffic) recoded by means of one edition only of a Multiple-Alphabet Table which had been in force continuously from early in 1937. By the outbreak of war, the enemy had, therefore, succeeded in substantially recovering both the basic book groups and the recoding Table, and he was able to read messages with little difficulty.

35. Between the 1st November, 1939, when a new Multiple Alphabet Recoding Table was made effective, and the 20th August, 1940, when the system ceased to be used consequent upon replacement by Naval Code with Auxiliary Vessels tables, a total of five successive editions only of Auxiliary Code Recoding Tables were used, and the enemy appear to have continued reading traffic with little difficulty. He captured a copy of the Auxiliary Code at Bergen in May 1940; a current recoding table also fell into his hands at the same time, but this edition was replaced by a new one on the 23rd May, 1940.

36. It is probable that the quantity of signal traffic with Auxiliary Vessels which became available to the enemy in the prolonged period when he was reading this Code, was of considerable assistance to him in his later successful attacks on the Long-Subtractor Auxiliary Vessels Table used with Naval Code, since the volume of material which

TOP SECRET

had been open to him from reading the Auxiliary Code helped him to assess the type of subject matter and phraseology normally encountered in signals to, from and between Auxiliary Vessels.

37. Inter-departmental Cypher. From about the beginning of 1939, the enemy had monitored traffic in the Interdepartmental Cypher, particularly in the Mediterranean, but at that time he had no clear understanding of the purpose for which this cypher was used. At the beginning of the War, traffic increased and analysis disclosed to the enemy that a long-subtractor system was used; owing, however, to the still small volume of traffic he was unable to break into it at the time.

38. In May, 1940, the enemy captured a copy of Interdepartmental Cypher No. 1 at Bergen. This edition had been in force since a considerable period before the war. Resulting from this "pinch" he was, from May, 1940 onwards, able to decypher messages even when the volume of intercepted traffic was less. Weekly Intelligence Summaries in this cypher sent by Admiralty to Naval Attachés abroad were read by him quite extensively. A great number of diplomatic messages was also decyphered; notably messages concerning political negotiations on military matters in the Middle East. It appears that in 1940, and in early 1941, the enemy also obtained from this source, information regarding disposition of certain of our heavy units (cruisers and above) in the Freetown Area. This was occasioned no doubt by exchanges of signals between ~~said~~ such units and military, R.A.F. and Colonial Authorities in West Africa.

39. Up till the middle of 1941, when Naval Shore Code was introduced, Interdepartmental Cypher had necessarily to be used for naval traffic between Admiralty (and other Naval Authorities) and Consular Officers, Reporting Officers, S.Os.(I) abroad, etc; it was also used as an Inter-service Cypher, since a special Inter-service Cypher was not available till June 1942. From this traffic, the Germans obtained considerable information on the routes of convoys and independently routed Merchant Ships in the Atlantic. They also read a number of our signals concerning German Auxiliary Cruisers which attempted (or were expected by us to to attempt) a break-out of South and Central American Ports. These were

TOP SECRET

largely, no doubt, signals exchanged between Admiralty and S.Os.(I) abroad, and which had necessarily at that time to be sent in Inter-departmental Cypher since the Shore Code had not yet become effective.

40. The time lag in breaking down messages in this Cypher was astonishingly short; the Germans say that messages could usually be read within six to ten hours of interception. The cypher was used with two long-subtractor series of Tables only, and at that time the General Recyphering Tables which carried the great bulk of traffic were changed at irregular intervals varying from about a month to as much as three months. Control of changes of editions was (and still is) vested in the Foreign Office, and having regard to the enormous distribution required, it was impossible then to introduce a rapid programme of changes. This, coupled with the fact that: (a) a relatively insecure Starting-point Indicator system was used, and (b) the bulk of messages were of a rather stereotyped nature, no doubt contributed to insecurity. It was owing to this suspected insecurity of Interdepartmental Cypher that Naval Shore Code was introduced on the 12th July, 1941, as the new medium for communication between Admiralty and Reporting Officers, S.Os.(I) abroad, Naval Attachés, etc., and, that the Inter-service Cypher was introduced for ~~the~~ three services use on the 25th June, 1942. Introduction of these two additional systems greatly curtailed the amount of information which had earlier been available to the enemy from this exploitation of Interdepartmental Cypher. From the middle of 1942 onwards, there is reason to suppose that the enemy profitted little from his work on this Cypher, and so far as Naval traffic is concerned the Germans eventually ceased work on the cypher altogether in December 1942. A new basic book, Interdepartmental Cypher No. 2 became effective on the 15th June, 1943.

41. Inter-service Cypher. This new Inter-service Cypher was brought into force for combined three-services traffic on the 25th June, 1942. The book is similar to Naval Cypher, and was used with long-subtractor tables until the 1st June, 1944, when the stencil subtractor system became effective. The enemy appears to have had little or no success in breaking into it.

TOP SECRET

42. Naval Shore Code. This Code was brought into force on the 12th July, 1941, and from then onwards was used (in place of Inter-departmental Cypher and G.T.C. recoded) for communications between Admiralty, S.Os.(I) abroad, Reporting Officers, and Naval Attaches, etc. The enemy apparently had little, if any, success with it, although he worked on it at intervals. Since most traffic in Shore Code has always been ~~recoded~~ raided by I/T, scarcity of intercepted messages, coupled with the fact that three separate Area Tables were used, made productive analysis difficult and scarcely worth while. Only a small start was made by the enemy at reconstructing the basic book groups. Note; the enemy was possibly discouraged to some extent from his work on Naval Shore Code by the very extensive use which was made of One-time Pads.

43. Anglo-French Code and Anglo-French Cypher. The four-letter Anglo-French code, recoded by bigram substitution tables, was used to a small extent for British-French communications up to the fall of France in June 1940. The enemy does not appear to have considered it worth-while seriously concentrating on the traffic. He captured a copy of the basic book at Bergen in May 1940. After the fall of France it was naturally assumed by us that the basic book was compromised; for lack of another, however, it had necessarily to continue in use (with new tables of course) for low-grade traffic with small Free French vessels without a Naval Liaison Officer. The Bigram Tables were replaced by multiple alphabet ones in May 1943, but throughout the war there is no indication that the enemy devoted attention to the relatively small and unimportant volume of traffic in this code.

44. The five-figure Anglo-French Cypher, recoded by long subtractor Tables, was used from late 1940 to the end of the War for a very small volume of traffic; mainly for communication with Free French warships in the Freetown Area. The traffic was so small that the enemy did not consider work on it justified. It is a remarkable fact that the Germans apparently never succeeded in obtaining from the Vichy French a copy of this cypher, which we of course assumed to be compromised after France fell.

TOP SECRET

45. Chronological Summary of German breaks into High-Grade Naval Book systems.

The following is a Precis of the salient features included on pages 63 - 74. It has been added in order to give a perspective view in brief of the main German successes referred to on those pages.

(a) Administrative Code and Auxiliary Code. - Both of these Codes were broken into before the war and were read extensively by the enemy up till the date they were withdrawn from use on 20th August 1940.

(b) Naval Code. - Edition No.1 was effective from 20th August 1940 and was broken into some six weeks later. Traffic broken was mainly that recoded by the Auxiliary Vessels' Tables, but some traffic in the Area I (Home and N.Atlantic) and General (world-wide) Tables was also read. Introduction of the Left and Right recoding procedure was comparatively little handicap to the enemy. From 20th January 1941 enemy successes greatly curtailed owing to use of disguised Starting Point Indicators, but following a return to plain Indicators on 1st September 1941 the previous standard of breaking was soon attained. Break in enemy successes on 1st January 1942 consequent upon introduction of Naval Code No.2. After about 10 days however, this edition was broken into and with increasing success until 15th December 1942 when disguised Indicators were reintroduced. This resulted however in a temporary setback only, and after a short delay Auxiliary Vessels traffic was again being read on a considerable scale. This continued until 1st March 1943 when Naval Code No.3 (an improved code) was brought into force and resulted in a break in enemy successes. By August 1943 however enemy was again breaking Auxiliary Vessels traffic and continued to do so with increasingly good results until 1st December 1943 when introduction of the Stencil Subtractor Tables put a final stop to enemy successes with Naval Code.

(c) Naval Cypher (Intra-R.N.Editions). - Edition No.1 had come into force in 1934 and was broken into before the war. It was read with a fair measure of success in the months immediately before outbreak of hostilities but a setback to the enemy was caused by introduction of new recyphering tables on 25th August 1939. By mid October 1939 however, it was again broken into. Enemy efforts were concentrated mainly on traffic in home waters. By Spring 1940 enemy work on the cypher had so far progressed that he read virtually all the traffic in connection with the Norwegian operations. Interruption in enemy successes took place on 20th August 1940 when Naval ~~Code~~ No.2 was brought into force. By the end of September 1940, however, he was again breaking a small proportion of intercepted traffic. Further setback to the enemy on 1st October 1940 resulting from combined effects of Left and Right recoding procedure and introduction of Area Tables. With increased staff, however, the enemy made progress rapidly but could not reach his earlier standard. Successes severely curtailed on 20th January 1941 by introduction of disguised Starting Point Indicators, and no breaks achieved for some four weeks; after this however it was again broken into but on nothing approaching the old standard. This state of affairs prevailed until 1st September 1941 when disguised Indicators were abandoned. Soon after this, the enemy again broke the cypher extensively, and before the end of 1941 had virtually recovered his old standard of before 20th January 1941.

TOP SECRET

(c) Naval Cypher (Intra-R.N.Editions) (contd)

This state of affairs continued until Naval Cypher No.4 was brought into force on 1st January 1942. The latter edition remained effective until 1st June 1943 and the enemy never achieved success with it comparable to that with the earlier editions. By March 1942 he broke into it to a very small extent, and by October 1942 he had made fair progress in reconstructing the basic cypher. In general, however, the intelligence available to the enemy from breaking traffic in this edition appears to have been negligible in comparison with earlier editions. Lack of enemy success with Naval Cypher No.4 can be attributed partly to fact that Naval Cypher No.3 (The British-U.S.edition- see below) was effective concurrently and attracted most of the enemy's attentions; partly also to the fact that from early 1942 onwards it had become possible to change editions of recyphering tables very much faster, and progressively increased use was being made of One Time Pads to recypher messages in the intra-R.N.editions of Naval Cypher. From 1st June 1943, when Naval Cypher No.5 became effective, until the end of the war, the enemy had no further successes with Naval Cypher.

(d) Naval Cypher No.3 (The British-U.S.Edition).- This edition was in force from before Pearl Harbour until 10th June 1943. From the time traffic in it first became heavy, late in 1941, the Germans devoted their greatest efforts to breaking it. It is unnecessary to recapitulate the effect on the enemy of the various cyphering procedures effective at different times; these have already been summarised in (b) and (c) above. It will suffice to observe that throughout the whole life of this edition the Germans maintained an outstandingly high degree of proficiency in breaking the traffic in it. During the course of 1942, there were times when the enemy was able to read up to some 80% of all traffic available to them. Often the Convoy traffic in the Atlantic could be read with so little time lag that the Germans had movement information from some 10 to 20 hours in advance. From early in February 1942 until the Cypher was withdrawn from use on 10th June 1943, the Germans could frequently read the daily Admiralty U.Bpat Disposition Signal, often as early as midnight on the day it was made. From 10th June 1943, until the end of the war, normal R.N.editions of Naval Cypher were used both for intra R.N. and limited combined communications and were not broken into by the enemy.

TYPEX.

Typex does not appear to have been seriously tackled by enemy cryptanalysts. From the time it was first used in 1939 for Naval traffic, material was, however, monitored chiefly to ascertain the extent to which the system was used and the proportion of high-grade book traffic which was turning over to Typex. The Germans did, apparently, examine the problem with a view to ascertaining the possibilities of successful attack, but, according to evidence so far available, it seems they decided that without a very much larger staff (which was not forthcoming), it would be futile to sacrifice profitable work on our book systems in favour of extensive analysis of Typex. A Typex machine, without drums, was captured during the 1940 French Campaign, together with a quantity of British Army Typex cyphering instructions and other related documents which disclosed the number and types of Drums used. Two, or possibly three, more machines, again without Drums, were also captured later during the North African campaign.

2. The Germans say they established by means of ordinary letter - statistics that the system was similar to their Enigma Machine; i.e. a method by which any given letter of the alphabet was changed on an average equally frequently into each of the other letters of the alphabet. According to statemen -ents by enemy cryptanalysts, they explored the possibilities of whether, if the drum wirings were to become known to them, they might be able to tackle the problem of breaking. But the question was not, they say, investigated in detail and since they did not possess any wired drums, the problem was allegedly treated as more or less of academical interest only. The Germans were aware tha Typex was used only between shore stations, and a further reason which they allege dissuaded them them from tackling it seriously was their (mistaken) view that Typex was used "predominantly for Staff and Administrative matters and was therefore of less importance for the conduct of the war". It is interesting to know that nondrums were ever captured by the enemy, since there was for a long time some uncertainty whether or not drums had fallen into their hands concurrently with the machines referred to in paragraph 1 above. From all the evidence available hitherto it seems safe therefore to assume that Typex traffic was never broken by the enemy. There is still, however, some reason to doubt whether or not we have learnt the whole story of enemy work on Typex.

TOP SECRET

3. Combined Cypher Machines. The Combined Cypher Machine first made its appearance purely for Limited Combined Naval communications in the Atlantic on the 1st November, 1943; it was extended for Combined (5-services) use on the 15th April, 1944, since it was important to have the system effective for use by all five services before the Assault on the Continent. It seems to have been only from the latter date that the Germans first turned their attention seriously to Combined Cypher Machine traffic. Material was collected by them and letter counts carried out on Hollerith. It is clear, however, that, anyway up to December 1944, the enemy had made no headway into breaking the system. The letter counts made by them showed frequency curves which corresponded well with one another but were not the same as those for Typex or the Hagelin machine. It is fair to assume that no messages in this system can have been broken by the enemy; he appears, indeed, to have advanced no further than arriving at the obvious conclusion that the first group of each message was the system (crypto-channel) indicator and the second group gave the machine setting.

PART II - SECTION B - LOW-GRADE SYSTEMS.

FLEET CODE.

The enemy worked on Fleet Code throughout the War with varying success, depending of course on the volume of intercepted traffic available to him in a particular edition. With an edition which remained in force for one month, it seems that he could normally achieve some measure of success after ten to fourteen days, but again this was dependent almost entirely on the quantity of material intercepted.

2. In general, little information of current operational importance seems to have been obtained by the enemy from this system. Some intelligence was obtained by him from reading traffic resulting from attacks on U-Boats in Home Waters and the North Atlantic, and also on the movements of United Kingdom coastal convoys. In the former case, however, the information accruing to the enemy was mainly of value only to the extent that it disclosed measures taken, or to be taken, by us when a U-Boat had already attacked a Convoy. No advance operational information was available to him. No current operational information of value appears to have been obtained by the enemy from the Fleet Code used during the North African Landings in November, 1942; this is probably due, in part anyway, to the fact that a special edition was set aside and used solely for that operation. The same applies in the case of the Assault on the Continent; in this instance the precaution had been taken well in advance of introducing fortnightly changes of editions, and this continued until the 15th July, 1944. The volume of material available to the enemy in Fleet Code was moreover greatly reduced on this occasion by reason of the use, for the first time, of Combined Assault Code.

3. In November 1942, the enemy captured in North Africa an edition of Fleet Code (No. 27) which had been set aside for use only as a practice edition, from the 24th November, 1942. This particular edition remained in force for exercise purposes until August 1944, and hence it transpires that the enemy was able to read a quantity of Fleet Code exercise traffic current in the Portsmouth Area before the Assault on the Continent. This traffic was, however, of no

TOP SECRET

operational importance in so far as plans for the final assault were concerned. One interesting example of lack of enemy success with Fleet Code, when the traffic was light, was his inability to exploit any Fleet Code traffic during the operation which resulted in the sinking of the "Sharnhorst" in December 1943. He intercepted some 30 of the signals made in Fleet Code during this operation, but although the Edition concerned was in its last few days of use, the enemy had, even by as late as 10th January 1944, been unable to produce results because "traffic on the other days was light". In this connection, however, it is noteworthy that Italian cryptographers, who were interrogated at Admiralty in February 1944, maintained that "50 to 100 messages were generally enough to break the Code sufficiently to get the sense of many messages".

4. A further sidelight in this connection is the apparent inability of the Germans successfully to break into the special edition of Fleet Code which was used during the Anzio assault in January, 1944. Although it transpires that by 1st February, 1944, the Germans had intercepted 158 signals made in this edition (signals in which were distinguished by a self-evident prefix), they had by then achieved no success, and it became apparent to them that there would only be the possibility of a break-in if the edition remained in use for a longer period. In point of fact, the edition was replaced very shortly afterwards.

5. There is, however, reason to believe that, by the closing stages of the war, the Germans must have greatly improved their technique in breaking Fleet Code. Thus, the following statement appears in one of the enemy's periodical Cryptanalytic Progress Reports, compiled at the beginning of March 1945: "Fleet Code - Despite the short period of validity of the code book, which is used unrecyphered, it is possible, by using increased staff, to obtain from the system findings of current operational value concerning anti-U.Boat activity and Coastal Convoys. About 1500 messages are decyphered monthly". It has already been observed in paragraph 1 above, that the enemy did, indeed, obtain intelligence from this source concerning ant-U.Boat activity and Coastal Convoys.....

TOP SECRET

convoys; whether or not, however, the figure of "1500 messages decyphered monthly" is an accurate one cannot be confirmed, it is an astonishingly high one, and if true, indicates that Fleet Code was used far in excess of what was thought to be (or indeed should have been) the case.

6. The enemy (both Germans and Italians) remarked on a number of cryptographic weaknesses in the construction of Fleet Code, the presence of which assisted them to break it. These are dealt with under the recommendations in Part III of this Review.

7. Combined Assault Code. The first edition of this three-letter code to be used operationally was No. 3 which was made effective for the Assault on the Continent in June 1944. It remained in use until the 20th June, 1944, and was then replaced by a number of subsequent editions used only for Limited Combined Naval traffic. The enemy succeeded in reconstructing a fair proportion of the groups in the various editions used, and reading a number of messages wholly or in part. These consisted mainly of times of arrivals and sailings of convoys and independently routed merchant ships between England and the invasion coast.

8. The code was used (or rather mis-used) extensively for weather reporting in Home waters, and the bulk of such messages appear to have been read easily by the Germans owing to their restricted and stereotyped texts; for this very reason, however, the breaking of the weather traffic was of little assistance to the enemy in recovering ~~of~~ other vocabulary groups. A Mediterranean edition of the Combined Assault Code was used for Operation Dragoon (Assault on South Coast of France), but due to scarcity of intercepted material it seems this traffic could not be exploited by the enemy.

9. There is nothing surprising in the enemy's successes with the Combined Assault Code. The security margin of such a code is of course low, and its use was, in the main, confined to urgent tactical signalling in connection with movements which could anyway not easily be disguised from the enemy.

TOP SECRET

Small Ships' Codes: LOXO, FOXO COFOX, MEDOX, TRAXO.

10. A summary of developments in the use of Small Ships' Signal and Operational Codes is included in Part I - Section B, of this Review.

11. The original, and simplest, code was the Small Ships Signal Code (LOXO) first introduced on the Home Station in August, 1941. The enemy experienced very little difficulty in breaking messages in this style of LOXO. The combined Code and Decode comprised words and phrases with two-letter groups arranged in alphabetical sequence of the first letter, and was particularly susceptible to attack. Each Daily Code changed at Midnight, and messages were often broken down in part by as early as 0400 or 0500; on occasions even by 0200 or 0300. The enemy attached considerable importance to reading this traffic in connection with his E-Boat operations in the Channel and North Sea.

12. Not until about June 1942 did the enemy capture an actual copy of a LOXO code. This "pinch" did not, however, contribute materially to the ease with which he continued to read the traffic, since comparison by him of the captured list of significations with the significations reconstructed analytically, showed that the latter was incomplete only in one or two respects.

13. The same system continued in use until the 1st December, 1942, when two editions were made effective concurrently, each being distinguished respectively by the prefix LOXOD (odd numbered edition) or LOXEN (even numbered edition). After a few days, the enemy found that use of the extra code made virtually no difference to the speed with which he could exploit traffic in both editions.

14. The next step was introduction of an improved style of LOXO code on the 1st August, 1943, incorporating many more significations to which were allocated three-letter, instead of two-letter, groups. The Code and Decode remained, however, a combined one with groups arranged in alphabetical sequence, and the enemy continued to read traffic almost as easily as before.

15. On the 1st September, 1943, there was introduced the first series of small ships' codes with hatted groups. This was the Small Ships' Operational Code COFOX, for use on the Home Station, and comprising two-letter hatted groups in a separate code and decode.

TOP SECRET

This resulted in a temporary setback to the enemy, but after about fourteen days he was able to achieve some success, and his work on reconstruction of this new type of code developed until, by early in 1944, he was again reading some 95% of intercepted traffic. The time-lag in breaking signals in this Code was always, however, rather longer than was the case with the old style of three-letter non-hatted LOXO code referred to in para. 14.

16. On the 1st April 1944, the "Small Ships Basic Code" was brought into force, using LOXO Coding Cards on the COFOX group system; i.e., three-letter hatted code and decode. The same system was applied to COFOX on the 1st October, 1944. The enemy's work was at first more difficult, and for assistance he had to rely largely on routine messages of a stereotyped nature (see, however, para. 23 below for work done by the enemy from February 1944 onwards on Exercise Traffic). Before long, nevertheless, he was reading a proportion of traffic coded by the new system. A time-lag of about five hours normally occurred before he broke into signals; after some twelve hours, however, most messages could be read.

17. The enemy always experienced difficulty in breaking into the code groups representing significations from the Numbers Table in the Basic Book; they were assisted however in doing so by the fact that numbers from that Table had necessarily to be used also for expressing the numbers allocated to Geographical significations.

18. Somewhat surprisingly, no copy of the "Small Ships Basic Code" appears to have been captured by the enemy. This was of little consequence, however, since he had, by cryptanalysis, succeeded in recovering ~~the~~ virtually all the significations in the code together with their respective numbered groups.

19. Although evidence on this point is not altogether consistent, it seems clear that, broadly speaking, introduction of the Small Ships' Basic Code with three-letter hatted coding cards did not materially hinder the enemy's work. At the most, it resulted in some hours extension of the time lag between interception and breaking. Gale warnings and Weather Reports made in the code were often of considerable assistance to him; also, after invasion of the Continent, the prevalence of very

TOP SECRET

stereotyped traffic from U.S. Patrol Vessels in the St. Malo area, which moreover helped the enemy by the practice of encoding serial numbers in their signals.

20. In the later stages of preparations for invasion of the continent, the enemy ascertained, from reading this traffic, the presence of Landing Craft on the East Coast; from the same source he was also able to trace movements of Landing Craft from Scottish bases to the South Coast. The aggregate of information obtained from such traffic gave him a very fair idea of the general dispositions of our landing craft in Home Waters. No movements or dispositions of Major War Vessels, nor of the Order of Battle for the forthcoming assault, were however deduced by him from this source. From the beginning of 1944, the enemy appreciated from reading this traffic that a noteworthy increase in Landing Craft tonnage took place in the Irish Sea, the Channel and the East Coast areas.

21. Material resulting from reading these Small Ships' Codes was carefully examined by the enemy in an endeavour to identify Delivery Groups; he had little, if any, success however in this respect owing to the very small number of messages in these systems which bore three-letter Delivery Groups.

22. Apart from the specific instances referred to earlier, exploitation of traffic in these Small Ships(Codes appears to have been chiefly of value to the enemy in affording him a general background of useful information into our M.T.B., Coastal Convoy, Mining and Minesweeping Operations in the Channel and on the East Coast. It is, however, noteworthy that one enemy "Report of Progress" goes further than this in saying that, by the end of 1944, work on Small Ships' Codes showed such successful results that it was possible to "obtain an insight, through these codes, into the plan and routeing of the Atlantic Convoys in Home Waters."

23. Comparable attention was paid by the enemy to the Overseas editions of Small Ships codes (chiefly MEDOX) used in the Mediterranean. Results were good at times, but on the whole more "scrappy" owing to breaks in the continuity of intercepted material. After the Autumn of 1944, indeed, it appears that the volume of intercepted material

TOP SECRET

from the overseas editions was so negligible that the enemy had no further success.

24. Traxo (Training) Cards. These Training Cards were first made effective at Home in January 1944, in order to practice small ships in the use of the new Small Ships Basic Code (see para. 16). They appear to have been used very little up to the end of January 1944, but from February 1944 onwards they were used extensively for practice traffic during the Landing Craft Exercises in the Channel which preceded the Assault. A proportion of such traffic was then broken into by the enemy, who, in doing so, profited also in as much as it assisted him in building up the Vocabulary of the Small Ships' Basic Code before the latter was brought into force operationally on the 1st April, 1944, for use with the new type of coding cards (LOXO, COFOX, MEDOX, FOXO).

25. There is of course nothing startling in the disclosures outlined above. The low security value of these necessarily simple codes has always been appreciated, and every precaution was taken to preclude their use for signals of primary operational importance. Recommendations for future policy regarding Cryptographic Aids for small ships are incorporated in Part III, Section B, of this Review.

26. Syko (Nyko) and Aircraft Reporting Code. Traffic, both in Syko and Nyko (Naval Cards), was covered by the enemy from the beginning of the war. To break either Syko or Nyko successfully, he needed some 40 or 45 messages, including one or two routine ones, on a Daily Card. The breaking of Syko was invariably easy since there was always a fair amount of intercepted material available. On one occasion, early in the War, the enemy obtained from a crashed R.A.F. aircraft all the Syko Cards for the current month and so was able to read that month's traffic at sight. This was valuable to him not only from the purely intelligence standpoint of the information obtained, but because it provided the enemy with extensive background knowledge of the type of subject matter and phraseology to be expected in signalling with Aircraft.

TOP SECRET

27. Nyko (Naval Syko Cards) was more of a problem for the enemy, since the volume of traffic was very low compared with that in Syko R.A.F. Cards, and it seems he was seldom in a position to intercept more than about ten messages a day. On one occasion, in 1942, H.M.S. "RENOWN" used Nyko whilst carrying out W/T tuning and testing at Gibraltar, and the enemy were able to locate the ship as being there because her name was spelt out in a number of messages.

28. It appears that, early in 1942, all work on Syko was transferred from the enemy's Naval Section to the G.A.F. Section; intelligence of Naval interest was passed by the latter to the Naval Section. The Naval Section resumed work, however, in the Autumn of that year in order to avoid delays in receipt of intelligence from the G.A.F. Section.

29. Enemy work on Syko and Nyko was greatly assisted by exercise traffic and routine weather reports. There were always, of course, more gaps on the right-hand side of the cards but never very many.

30. In July 1942, non-reciprocal Nyko and Syko cards were introduced ~~by the enemy's Naval Section~~ by the Enemy's Naval Section in an endeavour to achieve greater security, and from then onwards all work on both types of cards ceased for the remainder of the War. The G.A.F. Section continued, however, to work on Syko till the end of the War but without marked success after 1942, firstly because of the non-reciprocal cards, but chiefly because additional series of cards had been introduced (e.g. Coastal Command Cards from the 1st April, 1942) and, secondly, because Syko was replaced by the "Aircraft Reporting Code" on the 1st July 1943, for communication with shore-based Aircraft operating from the United Kingdom and Gibraltar. The G.A.F. Section worked on intercepted Aircraft Reporting Code traffic, but with very little success as there appears to have been insufficient intercepted material in this new type daily-changing three-letter hatted code to permit of its being exploited profitably.

Lettered Co-ordinates.

31. Recovery by the enemy of Lettered Co-ordinates from the S.P.02274 series (Tables of Lettered-Co-ordinates) was effected with considerable success in the early days of the War. This was undoubtedly due largely to the fact that editions of the Tables were then changed only at infrequent intervals. For example, during the period between the 1st December, 1940 and the 1st April, 1943 five editions only were used; i.e., an average "life" of some five and a half months per edition.

32. From the 1st April, 1943, monthly changes of these Tables were introduced, and from the 1st July, 1943, fortnightly changes, which continued until the end of the War. Recovery by the enemy was thereafter very much more difficult, although in narrow waters, such as the Channel, it was of course fairly easy for him to determine significations. In the Atlantic it was much more difficult; enemy D/F was not sufficiently accurate to give identifications of lettered-co-ordinates appearing in signals transmitted from mid-Atlantic.

Naval Aircraft Code

33. The Naval Aircraft Code (i.e. the Naval section of Air Force Code) when used plain afforded of course no security whatever, and instructions have always been that groups must be sykoed if some measure of security is desired. It is therefore interesting in this connection to observe that, according to the Germans, aircraft of Coastal Command used plain groups from N.A.C. for reporting on many occasions when it was clear that some security was required. So far as enemy interception was concerned, these reports were of course equivalent to plain language.

Slidex.

34. Slidex is a relatively simple Army R/T coding device used for concealing portions of a conversation which might be of value to the enemy. It was introduced late in 1943 and remained effective until the end of hostilities. It is mentioned here only because it was used in the Navy for R/T communication with Forward Observation Officers prior to and during Bombardment. It was broken very easily by the enemy, who state "decoding was often done with so little delay that messages could be dealt with like clear text in the evaluation".

TOP SECRET

PART II - SECTION C - MERCHANT SHIPS' SYSTEMS

From the beginning of the war, the enemy concentrated on breaking codes used for communication with Merchant Ships. Up till 11th January 1940, the only system in use for this traffic was the International Code with a Naval Appendix, groups from which were recoded by means of one Series only of simple bigram - substitution Tables. (Note: In the early stages of the war, private codes were also used by individual Shipping Companies). The enemy immediately recognised the importance to his Raiders of breaking into this system, and he had succeeded in doing so by as early as October 1939 (see also paras. 21 to 23 below).

2. On 11th January 1940, the International Code and Naval Appendix were replaced by the "Merchant Navy Code". This was a 4-letter code, also recoded by bigram-substitution Tables. Although the latter afforded only a low degree of security, the enemy experienced some difficulty at first as he was not in possession of the basic code. After some two months or so, however, he had succeeded in recovering numerous groups from the basic book and was able to make good inroads into the the new system. He was helped by the fact that, at that period, only one series of Recoding Tables (the General series) was used, and each edition had necessarily to be retained in force for some two months or, on occasions, even longer. In May 1940, the Germans had the good fortune to capture several copies of the new "Merchant Navy Code" at Bergen. Thereafter, his work was of course greatly facilitated and he was successful in reading the the bulk of intercepted traffic in the General Table with only a short time lag.

3. Recovered groups from the General Tables were passed by the enemy at once to special Monitoring Parties ("B" Groups) which he had established on board Raiders in the Atlantic, to assist the specialised cryptographic personnel comprising these Groups to read intercepted messages in Merchant Navy Code. Later, these B Groups were also established in enemy capital ships and cruisers, and their work was extended to cover traffic in Merchant Navy Code recoded by Independent Ship and Convoy recoding tables. There were, of course, breaks in the continuity of enemy successes, owing to ....

to changes of editions of recoding tables. As a rule it was seldom less than fourteen days after the introduction of a new General (or later, Indship) Table that the enemy could achieve profitable results, since the traffic was not usually heavy enough for an immediate break-in. Since, however, editions of these tables remained in force normally for about two months, and sometimes even longer, he had ample time ahead of him during which to exploit traffic before the next change of edition.

4. On the 10th October, 1940, a new series of recoding tables was introduced. This was the "Commodores Table", the first of a Multiple-Alphabet Recoding Table comprising 450 alphabets. The series was intended for use with signals to the Commodore of unescorted Convoys or to Commodores of escorted convoys when the latter had become separated from the escort. In practice, these tables were very little used until finally withdrawn on the 31st May, 1943, and there is no direct evidence of traffic in them having been exploited by the enemy.

5. From the 10th October, 1940, until the 29th May, 1941, there were in force together two series only of Merchant Ships' Recoding Tables; namely the General (Bigram-Substitution) Table and the Commodores (Multiple Alphabet) Table; traffic in the former continued during this period to be exploited successfully by the enemy.

6. On the 3rd October, 1941, the General (Bigram-Substitution) Tables were replaced by multiple alphabet (750 alphabets) ones. Although the latter system is, of course, more secure than bigram substitution, its introduction does not appear to have handicapped the enemy unduly, since he had already had considerable experience with the multiple alphabet system during the prolonged period when it was used for recoding the Auxiliary Code (see Part I, Section A). Starting points were not, of course, recoded, and the enemy had little difficulty in establishing whole or partial depths.

7. From the 23rd July, 1943, until the end of the war, the General Tables were long-subtractor (7,500 Gr.) ones for use with Merchant Ships Signal Book (Mersigs II). For reasons outlined later, however, the changeover to the subtractor system proved no obstacle to the enemy; in fact, used as it was on a compromised basic book,

his progress with the subtractor tables appears, broadly speaking, to have been more satisfactory than was the case with Multiple-Alphabet recoding, and the General Tables continued to be broken down by him, with virtually no time-lag, until the end of the War. Interrogation of enemy cryptographers regarding information obtained by them concerning British invasion preparations, discloses the fact that during the latter part of 1943, and early 1944, they were aware from reading messages recoded by these Tables that large quantities of Landing Craft were being transferred to the United Kingdom from the Mediterranean.

8. From the 30th May, 1941, there came into use another series of Multiple Alphabet (750 alphabets) Recoding Tables, namely "INDSHIP" Tables, for communication with slow unescorted merchant ships. This series remained in use throughout the war, but changed over to the long-subtractor system (7,500 groups per edition) from the 20th May, 1943 onwards. Like the General Table, these Indship tables received very wide distribution and heavy use; the enemy had therefore little more difficulty in breaking them than he had with the General tables. The eventual changeover to subtractor recoding appears to have achieved little, or nothing, in the way of added security, since the enemy had captured a copy of the new "Merchant Ships Signal Book" (Mersigs II) some four weeks before it came into force on the 15th April, 1942, to replace Merchant Navy Code. Exploitation by the enemy of INDSHIP Table traffic was, however, curtailed to some extent from the 20th April, 1944 onwards, from which date editions were changed monthly instead of every two months.

9. Convoy Tables. In 1941, two additional series of tables were made effective for use by individual convoys for the period of passage only. Initially, these were small Multiple- Alphabet Tables, each edition comprising 60 alphabets only. The first series (SHIPCON / later OUTCON Tables) was made effective for outward-bound United Kingdom to America Convoys on the 1st June, 1941; the second series (INCON Tables) became effective for Homeward-bound convoys in September 1941. These Tables were deliberately restricted in size

TOP SECRET

to 60 alphabets, since each edition was effective only for the period of passage of one convoy, and it was considered that tables of this length should afford sufficient security for the limited volume of traffic they might reasonably be expected to carry. In practice, however, the traffic carried proved to be larger than was anticipated, and often resulted in "depths" which enabled the enemy to break into a table and read details of routes given to stragglers; by this means he was sometimes able to collect data concerning the general course of the convoy concerned. These Convoy Tables were by no means, however, broken into on each occasion of issue of a new edition, since the volume of traffic was often insufficient for this purpose.

10. The convoy (INCON and OUTCON) Tables remained in use throughout the war. In 1943, however, editions were changed to subtractor ones, each comprising 150 groups. (Note: OUTCONs from the 18th January, 1943: INCONs from the 8th April, 1943). Since, however, the new Basic Code (MERSIGS II), with which these subtractor tables were used, had been captured by the enemy early in 1942 (see para. 8 above) and since (as was the case with the preceding multiple-alphabet tables) the traffic which they were required to carry proved heavier than was anticipated, the enemy succeeded in making inroads into these tables also. He soon became aware that each table comprised 150 groups only, and the first essential was to get a signal of more than 150 groups, in which case it was, of course, obvious that all basic-book groups over the 150 had been recoded by the same subtractor groups as the corresponding ones at the beginning of the signal.

11. Although it is clear that the enemy obtained a considerable amount of valuable information from exploiting traffic in these convoy tables, it is not possible to indicate his success in precise terms of individual Tables. Success depended, firstly, on the volume of signal traffic to an individual convoy, which was small if the convoy was unmolested but greater if attacked, and secondly to what extent overlaps in the table occured by reason of the haphazard choice of starting-points by different Originators. Having the basic code in his possession, the enemy could often read traffic in these tables on a depth of

two only: thus, if only two messages of some 20 groups each happen to have been recoded by means of the same subtractor groups, they could probably be read wholly or in part.

12. The enemy appears to have found it easier to break into these 150-group subtractor tables than into the preceding multiple-alphabet ones. Authentic differences were, of course, more readily apparent to him with a five-figure basic book (such as MERSIGS II which comprised some 20,0000 groups only out of the possible 100,000) than would have been the case with a four-figure book using all 10,000 groups. Information gained from reading these tables was particularly valuable to the enemy after the 10th June, 1943, since it was on that date that the British-U.S. edition of Naval Cypher (Naval Cypher No. 3), which the enemy had broken with marked success, ceased to be used and was replaced by Naval Cypher No. 5. From the 3rd December, 1943, onwards, however, use of secret lettered positions was made mandatory when quoting positions in signals recoded by the INCON and OUTCON tables, and this greatly reduced the operational value of results obtained by the enemy from this source.

13. It had meanwhile become apparent to the Admiralty that 150 subtractor groups were inadequate for these convoy tables, and enlarged editions comprising 750 groups each had been put in hand. These larger editions were first made effective for the INCON AND OUTCON series on the 13th April and the 21st May, 1944, respectively. This measure seriously hampered the enemy's work, and his successes were limited thereafter to a very much smaller proportion of traffic. Varying numbers of recoding groups were at times recovered by him from certain editions, but no longer all the groups of one table as had often been the case with the short tables.

14. Exploitations by the enemy of traffic in the convoy tables virtually ceased from the 1st September, 1944 onwards, from which date the larger tables referred to in the preceding paragraph were used in conjunction with a special "Diversion Code" incorporated as part of the Table itself and which, like the table, remained effective only for the passage of a convoy. The enemy failed to recover groups from the Diversion Code and from this date no further information respecting convoy routes and courses was obtained by him from the convoy tables.

TOP SECRET

His appreciation of convoy movements had, thereafter, necessarily to be deduced largely from Traffic Analysis and from such relatively unimportant information as he could obtain from reading traffic recoded in the General Tables (but see paras. 18 and 19 below).

15. In this connection, it is of interest to quote verbatim from an enemy Cryptographic progress report dated the 5th January, 1945: "The introduction of the Diversion Code on the 1st September, 1944, was a much more serious complication. This consisted of only two sheets, but is issued afresh for each convoy. All details on locations are given in it, and probably again in terms of latitude and longitude. Up to the present, this code has resisted all attempts at breaking with the small quantity of material available. In addition, the groups of this code cannot be included for purposes of comparison with others, and this hinders the breaking of other messages".

16. A curious, but from our point of view very satisfactory, feature of the enemy's work on Merchant Ships codes is his apparent neglect, until late in the War, to attempt exploitation of traffic recoded by means of "Oneship" subtractor pads. These pads were first introduced in August, 1941, for use in conjunction with a small five-figure Diversion Code, and were used for communications to fast independently routed Merchant Ships and oceangoing Tankers. From the 15th April, 1942, onwards, they continued to be used for the same type of traffic but with the new Merchant Ships Signal Book (MERSIGS II) as the basic code. The fact that a signal was recoded by means of one of these pads must have been apparent throughout to the enemy, since self-evident starting point indicators were used; moreover, up till the 15th November, 1942, the number of the Pad was expressed in clear at the beginning of the message. Despite this, the enemy appears, anyway up till late 1943, to have considered the pads as true "One-Time" ones, and hence that it was futile to attempt work on them. It was not until as late as May 1944 that knowledge obtained by the enemy of the manner in which the pads were used led to any measure of cryptanalytical success. It is true that it was the original intention to use these pads "One Time" only, but this was found to be impracticable, due to the impossibility of establishing proper control of the use of

TOP SECRET

starting points by the several different originating authorities all of whom required to make use of the same pad. In point of fact, the degree of security afforded by these pads had, for this very reason, occasioned the Admiralty some concern, and a large scale replacement programme for used pads was instituted. As an added precaution, moreover, it was prescribed from the 3rd December 1943, onwards that, when using Oneship pads, positions must be expressed in terms of secret lettered positions. These pads were used extensively for important signals to large independently routed merchant ships, including troop transports, and although it is true that from May 1944 onwards the enemy devoted attention to breaking into them, it seems, from the evidence available, very doubtful if he achieved any marked success.

17. The successful exploitation by the enemy of traffic in the General and Independent Ship recoding tables is not surprising. The security value of these tables has always been known to be very low indeed; it could not be otherwise with tables having such a wide distribution and carrying loads of traffic which could not be satisfactorily controlled due to the impossibility, for administrative reasons, of instituting changes of editions at a rate commesurate with the volume of traffic prevalent over specific periods. Enemy successes with the earlier short multiple-alphabet and short (150 group) subtractor INCON and OUTCON Tables is also no longer surprising in the light of knowledge which was later at our disposal respecting the security of both of these recoding systems when used with a compromised basic code. Further comments on this matter have been included in Part III, Section C, of this Review.

18. In conclusion of this section, the following extract is quoted verbatim from an enemy Cryptographic Progress Report of the situation obtained at the beginning of March 1945:

> "Merchant Navy Code - 2,000 messages in this system are decyphered monthly and completely read; the basic book is held. The most important operational results obtained from it are:-
>
> (a) Times of arrival of Atlantic Convoys in British and U.S. coastal waters, as well as distribution

of ships among ports of destination. This permits far-reaching conclusions to be drawn regarding convoy time-tables.

(b) Successes, as and when they occur, of attacks by our U-Boats, as well as damage to and losses of merchant ships at sea.

(c) Approach points for convoys and independently routed ships (Irish Sea to Port Said).

(d) Insight into the number of ships routed independently, and solution of ships' secret call signs, which are of assistance in traffic analysis.

(e) Weather reports from the Channel, Biscay, Mediterranean and Indian Ocean."

19. This catalogue of successes is an alarming one, more especially when it is appreciated that the results were obtained almost exlusively from reading traffic in the widely-held General and Independent Ships' Tables which, on account of their known insecurity, were used only when no more secure system was available. At the time this Progress Report was written by the enemy, he was no longer breaking into our Convoy Tables (see para. 14 above), and it is easy therefore to conjecture how much greater must have been the sum total of intelligence available to him before the wholly secure Convoy Tables were introduced on the 1st September, 1944.

20. The enemy appears never to have captured any Merchant Ships' Recoding Tables from British or Allied ships; nor were any copies of Merchant Ships' Signal Publications obtained by him from Neutral sources such as Neutral ships trading in the Allied interest.

TOP SECRET

21. Monitoring Parties ("B.Groups") - An interesting side-light into German work on our Merchant Ships' Code traffic,in the early days of the War, is afforded by a Berlin report of 23rd March 1940 dealing with activities on board the Tanker ALTMARK during her cruises in the North and South Atlantic in the latter part of 1939, whilst acting as a refuelling ship for the GRAF SPEE.

22. Monitoring Parties, or "Intercept Groups" (B-Groups - see para. 3 above), were estanlished in the GRAF SPEE and the ALTMARK. The work done by the ALTMARK Group supplemented that done in the GRAF SPEE, and up till the time the latter was scuttled in December 1939, material intercepted in the ALTMARK was handed over to the GRAF SPEE whenever there was a rendezvous between the two ships.

23. From 18th October 1939, transmissions to British Merchant Ships from Rugby, Freetown, Falkland Is and Capetown, and traffic on 500 k/cs generally, was monitored regularly on board the ALTMARK.

At this period, the system used was the International Code of Signals with Naval Appendix and simple substitution recoding tables (see.para. 1), which had been broken down by the enemy, and the report states that all Merchant Ships traffic from the above Stations was read. An example is quoted of a coded message to all British Merchant Ships on the sighting and reporting of the ALTMARK, with a description of the ship, which was transmitted from Rugby and intercepted and decoded in the ALTMARK. In general, the contents of the decoded messages comprised instructions to British Merchant Ships about putting into harbours, and re-routeing orders. From this source the Germans ascertained the forthcoming introduction (on 11th January 1940) of the new Merchant Ships Code to replace the International Code. Up till 10th January 1940, all the (International Code) messages could be decoded in the ALTMARK, but following the introduction of Merchant Navy Code on 11th January 1940 no further messages could be broken, and on 20th January 1940 the ALTMARK ceased to intercept the Merchant Ships traffic.

It transpires from the same report that up till 23rd March 1940, Berlin had not succeeded in breaking into the new Code.

TOP SECRET

PART II - SECTION D - CALL-SIGNS AND DELIVERY GROUPS.

Before remarking on enemy successes, it is desirable to recapitulate briefly the main systems used during the War.

2. Major War-Vessels. From the beginning of the War till the 14th October, 1941 - three-letter unrecoded call-signs and Delivery Groups, published in two separate series. Call Signs: S.P.02218 (editions changing approximately every two months). Delivery Groups: S.P.02198 (editions changing approximately fortnightly). From the 15th October 1941 till the 14th July 1942 - Composite monthly-changing editions, S.P.02396, containing three-letter call-signs and Delivery Groups: the Delivery Groups were recoded by means of a daily changing simple substitution table, but applied only to the 2nd and 3rd letters. From the 15th July, 1942 till the 31st January, 1944 - As above, but all three letters of Delivery Groups were recoded. From the 1st February, 1944, to the end of hostilities - New system comprising two publications; Part I: List of Ships and Authorities with five-figure Key-Numbers, editions changing half-yearly (S.P. ~~2535~~ 1489); Part II: three-letter call-signs and Delivery Groups associated with Key-Numbers from Part I, and with daily changing index-numbers applied to Delivery Groups Key Numbers (S.P. ~~2536~~ 2490); editions changing monthly.

3. Minor War-Vessels. Throughout the War - International Signal-Letters, recoded by simple substitution tables changing monthly and incorporated in S.P.2253, editions of which remained in force for six months.

4. British U.S. Until the 1st July, 1944 - Unrecoded letter-figure-letter-figure call signs (used also as Delivery Groups) from S.P.02378 series. Editions remained in force for prolonged periods varying from about four months to as much as a year; average life of an edition was approximately seven months. From the 1st July, 1944, to the end of hostilities - Identic system to the new Major War-Vessels one effective since the 1st February 1944 for British use (see para. 2 above), except that call-signs and Delivery Groups remained letter-figure-letter-figure ones.

TOP SECRET

5. Merchant Ships. Throughout the War - Secret call signs allocated to International Signal Letters and issued in "Mercantile Secret Call Signs" (S.P.02182). Spare blocks of secret call-signs were provided in this publication and were allocated when an existing call sign based on the ship's Signal Letters was known, or suspected, to be compromised.

6. Enemy Successes. From 1940 onwards the enemy worked on registration and evaluation of Delivery Groups and call signs.

7. Major War-Vessels. Positive identification by name of ships and authorities with their respective Delivery Groups was achieved to some extent up till the 10th June, 1943, not from breaking the Delivery Groups themselves but from cryptanalytical success with Naval Cyphers and Naval Codes: i.e., from reading the codress and hence identifying the Delivery Groups appearing on the same message. Some measure of success was achieved by the same means between September 1943 and the 31st December, 1943, from breaks into Naval Code, but nothing thereafter.

8. The enemy was aware that an entirely new system was introduced on the 1st February, 1944, for British Major War Vessels, and on the 1st July 1944 for British-U.S. use, but he could only conjecture upon the nature of the system; all methods of approach proved valueless. He subsequently captured an "S" Order describing the new system and also elicited full details of it from prisoners captured from the Canadian Destroyer ATHABASKAN sunk on the 29th April, 1944. ~~He subsequently captured an~~ From the knowledge so obtained, he formed the opinion that without possession of the publications themselves, endeavours to break into the system would be futile.

9. When positive identification was impossible from decyphering the codress, work proceeded on the lines of analysing Delivery Groups appearing on different W/T Services, and endeavouring to associate them with their true significations. With Delivery Groups remaining constant throughout the life of each edition, as was the case up till the 15th October, 1941, considerable success was achieved. Introduction from that date

TOP SECRET

of the daily recoding process for the second and third letters was a set-back, but only for about twenty-four hours. The subsequent recoding of all three letters proved a greater stumbling block but was also rapidly overcome. The enemy could make no attempt to establish the actual signification of individual Delivery Groups; he could, and did, however, achieve considerable success in establishing the day to day relationship between identical basic Delivery Groups, by means of building up the daily- changing substitution code in the form of constant relationships between true and recoded letters. He took zero day as the day a new edition of S.P.02396 became effective, and the recoded Delivery Groups appearing on that day were treated as relative basic groups upon which to construct "synthetic" keys for the following days. This procedure continue until further efforts were frustrated from the 1st February, 1944, by the introduction of the new Key-Numbers system.

10. Minor War-Vessels. Positive identification of the Minor War-Vessels Call-Signs (which were, of course, used also as Delivery Groups), was established with a large measure of success throughout the war. This was due partly to the low security of these call signs, which for a month at a time remained directly associated to the Signal Letters of the vessel concerned, and the substitution keys for which were broken in a few hours. From his cryptanalytical successes with the Auxiliary Vessels Recoding Tables, the enemy was also in a position to determine, from the codress, the positive significations of numerous Minor War Vessels Call Signs (used as Delivery Groups).

11. British-U.S. Successful exploitation by the enemy of traffic in the British-U.S. Naval Cypher (No. 3), which continued in use from the entry of America into the War until the 10th June, 1943, enabled him largely to reconstruct the plain (un-recoded) call-signs in the original S.P.02378 series. This reconstruction assisted him, in turn, by expediting the decyphering of the signals themselves, since having, for example, already interpreted the call sign R2H7 as "C.T.G.25.6" he could fit the latter

TOP SECRET

authority into the codress. His success with British-U.S. call signs was brought to a conclusion on the 1st July, 1944, when the new system of Key Numbers was made effective also for British-U.S. communications.

12. Merchant Ships. Secret call signs from S.P.02182 series ("Mercantile Secret Call Signs") were broken fairly often from the decoding of traffic in Merchant Navy Code and, later MERSIGS II, since the names of the merchant vessels addressed were frequently included in the subject matter of the coded signals. The precise degree of recovery of these call signs is not apparent, beyond a statement by the enemy that he "had a card-index of quite a lot of steam-ships."

TOP SECRET

PART III - GENERAL CONCLUSIONS, LESSONS LEARNT, AND RECOMMENDATIONS FOR FUTURE POLICY.

SECTION A - HIGH-GRADE SYSTEMS.

BOOKS.

War experience has fundimentally altered earlier conceptions of the degree of security afforded by figure codes and cyphers recoded by the subtractor method.

2. Enemy successes, and in particular his skill in exploiting traffic in the British-U.S. Naval Cypher (No. 3) recyphered by the long subtractor system, has proved conclusively that, except of course when a One-time pad is used, the subtractor system may only be considered reasonably secure against skilled scientific attack: (a) if the volume of traffic carried by a specific block, or list, of subtractor groups is far more rigidly controlled than was originally thought necessary, (b) if the security of the basic-bode groups themselves is very carefully safeguarded by frequent changes of editions, coupled with security improvements in the design of basic books, and (c) if a thoroughly sound system of Table and Disguised Starting Point Indicators is used.

3. The foregoing provisos apply, of course, a fortiori to recoding by means of the old type of long-subtractor tables which are now fortunately obsolete in so far as Naval High-Grade systems are concerned. They should, however, be looked upon as no less important in considering the future developments of the stencil-subtractor method of recoding, since even assuming, for example, the absence of "presented depths" which might be achieved by an "unbreakable" indicator system, there remains the fact that expert cryptanalysis may disclose "depths" from the discovered presence of repeats and differences. In this connection it is perhaps appropriate here to quote, as a "danger-signal", the following extract from an enemy Cryptographic Progress Report written in March 1945; "In contrast to the diminishing prospects of getting hold of a copy of the basic book, detailed study of the Naval Cypher/Naval Code recyphering system revealed, during the last few months, certain important weaknesses in the system, and new lines of approach were recognised which point to the probability of a break-in even without having the basic book."

TOP SECRET

4. Since, clearly, there can be no question of reverting to the obsolete long-subtractor system for Naval High-Grade book traffic, the following comments refer to the Stencil Subtractor system.

5. Control of volume of traffic on Inidvidual Key Sheets. Although the average daily load of traffic, taken over a period of one month, can in the long run be controlled with reasonable success by the introduction of additional series of Tables, no satisfactory answer has been found to the problem of eliminating traffic peaks on particular days and which may well result in the presence of dangerous "depths" on those days. Granted that future policy will result in Machine Systems replacing the book systems as the standard form of Naval high-grade cryptography, this danger will be largely eliminated; since, however, it is to be expected that the Stencil Subtractor system must remain as a standby for machines, the problem is one which merits serious consideration.

6. Rates of change of editions of basic books. The governing factor must of course remain the load of traffic carried. War experience showed the importance of changing editions at an absolute maximum of six-monthly intervals. If the War had continued much longer it had been planned to reduce the life of editions of Naval Cypher and Naval Code to four, or even three, months.

7. Improvements in the design of basic books. Resulting from War experience a number of security improvements have already been incorporated in Naval Cypher and Naval Code. There is scope, however, for further improvements. A notable weakness in the earlier editions was the inadequate provision of alternative groups for the most commonly used significations. This has been partially remedied in current editions, but the security advantage of having a liberal choice of alternative groups is so great that the procedure should be extended. The difficulty has, of course, always been one of insufficiency of available groups for Part I of a four-figure book. This could be overcome by the exclusion from Part I of all significations other than those for the vocabulary and Amplifying phrases, coupled possibly with pruning from the vocabulary itself of all significations which a careful analytical survey show to be rarely used. The Spelling Table could be removed and incorporated in another of the existing Parts, or in a separate Part of its own. (Note: This will anyway be desirable for the

TOP SECRET

reasons given in para. 8 below).

8. Spelling. It has always been a difficult problem to devise a cryptographically sound method of spelling those words which cannot be incorporated within the necessarily restricted scope of a four-figure group/Vocabulary. The "Single Letter Spelling Table" was discovered to be thoroughly unsound, and was discontinued in April 1941. The "Syllabic method" now used (in conjunction with a bigram spelling table) is likewise unsound. There is conclusive evidence that it afforded the enemy substantial assistance, since if he had succeeded in recovering the basic group for the signification comprising the first part of the spelt word, he was often, and with a reasonably degree of certainty, able to guess the nature of the complete word being spelt, and so to recover the one or more succeeding groups representing significations for the complete word spelt. The most satisfactory answer to this problem appears to be discontinuation of the syllabic method of spelling, and provision instead of an extensive spelling table incorporating not only bigrams, as at present, but all the more frequently encountered trigrams and commonly used word-beginnings and endings. Ample alternative groups should be made available in this spelling table for the more frequently used letters, bigrams and trigrams. Groups at present allocated in the short bigram Spelling Table are common to all parts of the Book; this will, of course, be impracticable with the greatly enlarged Spelling Table envisaged, and although disadvantageous from the point of view of rapid handling, the alternative must be arrangement of the Spelling Table in a separate Part of its own.

9. Geographical significations. The system at present in force, by which identical groups in Part I of the Basic Book are provided both for a Vocabulary and Geographical (or Proper Name) signification, is unsound and proved of considerable value to the enemy cryptanalyst. Since, for obvious reasons, the Vocabulary and the Geographical significations were related to one another so far as practicable in alphabetical sequence, the enemy could, if he had succeeded in recovering a basic Vocabulary Group, form a reasonably accurate assumption of the corresponding Geographical signification, and vice versa. This system has been discontinued in future editions of Naval Code and Naval Cypher,

and a separate part has been devoted to Geographical and Proper Name significations. This criticism is therefore included as a reminder that on no account should the old system be resumed.

10. "Ship Index" - There is conclusive evidence that the enemy profited from the use, over a long period, of one and the same edition of the "Ship# Index"; i.e., the use, concurrently with changing editions of basic cyphers and codes, of standard non-changing four-figure groups provided for warship significations in the "Ship Index." This method of coding names of warships not appearing in the lists in the basic books should be discontinued. Names of warships for which groups are not available in the basic book should be coded by means of "L.N. Numbers."

11. Indicator systems. A thoroughly sound Table and Disguised Starting Point Indicator system is an obvious pre-requisite to the security of subtractor recoding. The plain (undisguised) Starting Point Indicators used with long subtractor tables up to the 20th January, 1941 and again, in a modified form, from the 1st September, 1941, to the 15th December, 1942, provided the enemy with valuable assistance. So far as Table Indicators are concerned, the present system appears adequate. If, however, full value is to be obtained from a Table Indicator Book such as the S.P.02169 series, endeavour should be made to assimilate Minor War Vessels into a Call-Sign and Delivery Groups system effective also for Major War Vessels. Hitherto, use of distinctive call-signs for Minor War Vessels has virtually nullified any security advantage attached to the use of Table Indicator groups denoting the use of Auxiliary Vessels Recoding Tables. A like state of affairs obtained in the case of British-U.S. Recyphering Tables, since use of one or other of these few series was necessarily advertised to the enemy by the accompanying and distinctive British-U.S. Call Signs and Delivery Groups. The need for well disguised ("converted") Starting-point Indicators with the Stencil Subtractor system of recoding is exemplified by the success achieved by the enemy in breaking into the single-conversion procedure and the ingenuity displayed by him in evolving a method of attack on the double conversion procedure. (See part II Section A.)

TOP SECRET

12. MACHINES. All the evidence available confirms that the enemy never succeeded in breaking into traffic in Typex or the Combined Cypher Machine. This is, of course, no guarantee that, given favourable circumstances, he might not have achieved some success; in practice, however, it is clear that he did not dispose of sufficient skilled personnel beyond that necessary to conduct a fairly cursory examination into our machine systems, and from this to convince himself that, with the limited means at his disposal, chances of successful exploitation were very small. He decided therefore that it would be unprofitable for him to divert his attentions from Book to Machine systems.

13. After review of all the present known facts and factors touching the respective merits and demerits of high-grade book and machine systems, there is no escaping the conclusion that well designed and properly used machines afford a higher degree of security than does a book system subject to any but a one time subtractor recoding process. Apart, however, from the security aspect, machines must for practical considerations eventually supplant book cyphers and codes as the Navy's standard high-grade cryptographic system. Whilst Books would no doubt suffice under peace conditions, only by extensive use of machines could War time traffic volumes be dealt with satisfactorily. This is not of course to say that high-grade book systems can be dispensed with entirely. A standby system must obviously remain available for use on occasions when machines are not held or are inoperative. This can best be provided by retention of one basic book (Naval Code) used with several series of Stencil Subtractor recoding tables. Moreover, retention of a book system is essential in order to fully to exploit the simplest and most flexible known means of achieving 100% security; namely use of One Time Pads.

14. There is, however, wide scope for improvement in the design of the present Cypher Machine (Typex Mark II) before mechanical cyphering can properly be accepted as the mainstay of Naval cryptographic communications. The machine now in general use is largely obsolete in design and suffers from numerous disabilities both from the point of view of security and of practical handling. It is prone to

TOP SECRET

a variety of mechanical faults which not infrequently result in complete breakdown. Moreover, Typex operation has been complicated in recent years by the progressive introduction of numbrous and tiresome procedures and restrictions which the operator must bear constantly in mind in the interest of security. What the Navy requires, and must press for, is a machine which, whilst providing the highest possible security, is nevertheless reasonably simple to operate and maintain in good running order. The Typex Mark II machine is far from reaching this standard. The machine of the future should be so designed as to eliminate the need for "special procedures" by the operator, and to reduce the frequency of changes of machine (drum) settings to an absolute minimum consistent with security. Its mechanism should be simpler and more robust than that of the Typex machine, and so constructed as to function equally well in varying extremes of temperature and humidity. It is probably unreasonable to suppose that, for general intercommunication purposes throughout the Fleet, a machine could be evolved to provide complete "One Time" security; it would, however, be of enormous advantage if the future machine were so nearly to approximate "One time"security as to allow of the publication, when necessary, of the literal texts of cyphered messages, and the reference in plain language signalling to the date time groups and/or subject matter of encrypted messages.

15. One Time Pads - It is recommended that the existing procedure for use of One Time Pads should be modified in the interests of simplicity and flexibility. Navy Two, Three, Six and Twenty series of pads should no longer be produced in the form of "OUT" and "IN" Pads, since this tends unduly to complicate their distribution and use. It is, moreover, undesirable from the accounting aspect since numerous pads held by different authorities bear identical registration numbers.

16. Apart from a different copy number, each pad of the same series should be identical in every respect. Pads should be divided into sections of an equal number of pages each, each section for use by a specified originator only. If one particular originator were likely to require more pages than the remainder, he would be allocated two or more sections in the case of the Navy Six or Navy Twenty Pads.

TOP SECRET

On the cover of each Pad should be printed the list of Lettered Sections contained therein, and the numbers of the pages allotted to each section. Against each Section letter there should be a space to be completed in manuscript with the name of originating authority to whom the Section is allocated.

17. Navy Two and Navy Three series pads could remain their present size, i.e. 100 pages. In order, however, to provide sections of adequate length, Navy Six pads should be increased in size to 200 pages and Navy twenty pads to 400 pages. To reduce their bulk, all pads could be produced in the style of the old long-subtractor tables; i.e. groups printed on both side of pages, but the groups (and hence the pages) could be smaller, and the pages thinner, since each would be used once only.

18. The system described above would not be practicable for "Navy 50" Pads. It is doubtful, however, whether in practice such a series will continue to be a requirement, but if so, a pad should comprise one Section of 100 pages only and its use should be restricted to one way traffic <u>from</u> a Senior Officer or controlling authority.

19. A new series of One-Time Admiralty Code Out Pads should be instituted and distribution extended to <u>all</u> Major War-Vessels in <u>all</u> areas.

20. <u>General.</u> The adoption of the American six-figure date-time group procedure resulted in a cryptographic weakness which assisted the enemy in breaking into long-subtractor tables.

TOP SECRET

PART III - SECTION B - LOW-GRADE SYSTEMS .

Fleet Code.

Broadly speaking, this book appears to have met the requirements for which it is designed; namely, a necessarily low-grade but simple and rapid system for tactical intercommunication. Certain weaknesses in its design, however, coupled with opportunities for its improper use by unskilled or negligent coding personnel, facilitated the work of the enemy cryptographer and should be eliminated so far as practicable.

2. Production of editions should be accelerated in War to allow of automatic fortnightly changes whilst providing a reserve for additional intermediate changes preceding and following important operations. It is recommended that editions should no longer be produced by Letter-Press but rather in multigraph form similar to the Combined Assault Code.

3. Resulting from the limitations imposed by a three-letter code, alternative groups have not hitherto been allocated for the more commonly used words and phrases; e.g. "Attack", U-Boat","Aircraft," "Enemy", "My position course and speed", "Have sighted", etc. Nor, indeed, are even single groups provided for such frequently used phrases as "Have attacked U-Boat, in position", "Have been attached by enemy Aircraft", "Have sighted enemy aircraft, bearing", etc., etc. A thorough analysis should be made of a cross-section of Fleet Code Exercise traffic, and, in the light of the resulting frequency tables, the Vocabulary and Distress Phrases Sections should be re-edited to include important additional significations. Alternative groups should also be made available to the greatest extent possible. Sufficient extra groups for this purpose could possibly be found by removing the Section devoted to Foreign Warships, and pruning the existing vocabulary in the light of results obtained from the analysis. A cursory examination of the existing Vocabulary discloses the presence of many significations which it is safe to assume can seldom, if ever, be needed. A very substantial quantity of additional groups could also be obtained if the "A.B.C. Tables" were abolished (see later).

TOP SECRET

4. There is evidence that assistance was afforded to the enemy by incorrect use of the Code to the extent that positions were often expressed by groups taken from the Numbers Table, or from the Minutes Table included under "References to Previous Messages". This is, of course, contrary to the instructions for using the Code, but no doubt a contributory cause was the introduction of the American six-figure date-time group procedure which is not catered for in present style editions. It would be of advantageous if future editions were to incorporate a separate Table for coding these six-figure groups (by means of three groups each representing two digits). Instructions for handling the Code should include a specific warning against the use of the Numbers Table or the Date-time Groups Table for coding positions, and should stress that for the latter purpose use must be made only of the Position and Compass Table. Similar warnings should be printed at the head of each of the three Sections concerned.

5. Spelling. The system of spelling is criticised as a source of weakness both by German and Italian cryptographers who stated (quite independently of one another) that entry into the Spelling Table was facilitated by use of a standard "set" of single letters, bigrams and trigrams each of which was provided with one group only. A separate Spelling Table is not, in fact, incorporated in the present style of Fleet Code, but spelling groups are included in alphabetical sequence within the Vocabulary itself. So far as cryptographic weakness is concerned, however, the ultimate result is, of course, the same. The difficulty of evolving a cryptographically sound spelling system has already been commented upon in Part III, Section A, of this monograph, and the same views hold good to an even greater extent with Fleet Code, owing to the scarcity of available three-letter groups. Short of incorporating a separate section in the Fleet Code devoted exclusively to an extensive spelling table with numerous alternative groups (and this is undesirable from the practical handling viewpoint), there is no satisfactory answer to this problem. It was the frequent spelling out of names of merchant ships which afforded the enemy most assistance in breaking into the spelling groups; he often needed only to recover one, or possibly two, of the spelling groups and was then able to guess the name of the ship

TOP SECRET

concerned and so recover the remaining spelling groups. This weakness could, admittedly, be overcome by coding the names of merchant ships in two groups by means of their International Signal Letters. This procedure was used early in the War but was discontinued because of the incidence of corruptions. It is, however, for consideration whether it should not be resumed in the case of Fleet Code since the overall gain in speed and added cryptographic security would probably outweigh the added risk of occasional corruptions.

6. A.B.C. Tables. It is doubtful whether the Fleet Code method of recoding groups and single flags, pendants and signs from the Fleet Signal Book and the A.V.S.B. will continue to be a requirement in the post War Navy, when rapid tactical intercommunication between fleet units is more likely to develop along the lines of VH/F, or R/T with voice-scrambling devices. If the A.B.C. tables could be dispensed with, a large quantity of badly needed groups would be released for use elsewhere in the Code. The enemy was well aware of the purpose of these A.B.C. groups, but does not appear to have given them particular attention; he stated that it was sometimes possible to identify the Senior Officer's Ship as being the one which originated most signals using these groups.

7. Small Ships Codes. It will have been apparent from Part II, Section B, of this Review that our system of Small Ships Signal and Operational Codes, although satisfactory from the practical signalling aspect, is basically unsound from the point of view of achieving even short-term security. Perhaps the best that can be said of the system is that it was the most satisfactory one which could be devised with the means then at our disposal, and that at least it represented a substantial advance from Syko.

8. The future policy regarding cryptographic aids for small craft requires, therefore, to be examined with great care and approached from a new angle. The problem is no easy one, since in this sphere of communications the conflicting requirements of simplicity and security are paramount. Obviously, however, it will be futile to perpetuate a system with such proved shortcomings, and which is particularly dangerous in the hands of personnel who are not constantly alive to its security

TOP SECRET

limitations and in whom may well therefore be engendered a false sense of security which they think to be provided by using "a code". Indeed, in such circumstances it is hardly an exaggeration to say that plain language is often preferable, since originators would then at least be alive to the necessity for extreme caution.

9. It is urged that no attempt should be made to retain the present system, bolstered up in the form possibly of a better Basic Code and additional series of Coding Cards. The very nature of the system is unsound, and it is extremely unlikely that palliatives such as those mentioned would achieve the desired result in the face of expert cryptanalytical attack.

10. One or other of two alternative systems are recommended for trial, viz:

(a) Use of a simplified model of electric cyphering machine, operated manually and equipped with a low-power electric cell to provide the necessary current through the scrambler mechanism. There are three types of such machine available for trial in small craft; namely the ex-German "Enigma" Machine, and the small Typex models Mark I B and Mark VI.

(b) Use of a basic four-figure code in conjunction with stencil-subtractor recoding tables.

11. Important considerations to be borne in mind when deciding upon a future system for small craft, are, firstly, that compromise by capture of the basic system (i.e., the machine and all its components, or the basic book) must from the outset be assumed to be inevitable. Restoration of an adequate standard of security must, therefore, (and in fact probably can) be achieved solely by introduction of new Key Documents for use with the machine, or new Tables for use with the basic book. Secondly, if a machine is to be used, operating procedure must be simple, and the operator must be freed from a plethora of special rules and restrictions such as those now applicable to the standard Typex Mark II or Combined Cypher Machines used ashore and in larger vessels. If, on the other hand, the book system is used, then the basic book should be classified only as a Book of Reference, and the recoding procedure should be simplified to an extent commesurate with the limited degree of security necessary for such a system. It is particularly important that the Indicator system should be free from an unduly complicated conversion (disguised) procedure.

TOP SECRET

12. Neither of these two systems will, of course, be so easy for small craft to handle as the LOXO type of Small Ships Code, but faced with the knowledge now at our disposal, we can no longer afford to sacrifice security for simplicity to the extent prevailing hitherto. Added complexity in cryptographic devices must be accepted as inevitable and co-incident with the numerous other mechanical complications associated with the progress of modern warfare.

13. Syko, Nyko. There is little scope for useful comment on the Syko system of coding. The cryptographic weakness of this method is also fundimental, and there are scanty grounds for supposing that it can be overcome to an extent which would warrant its retention.

14. So far as intercommunication between small craft is concerned, Nyko should be replaced by one or other of the systems advocated in the preceding paragraphs. If, however, machines are introduced for use in small craft, a standby system will be essential and this might take the form of Nyko.

15. For communications to and from Naval Aircraft, it should be possible to replace Nyko by daily changing hatted three-letter codes similar in style to the Aircraft Reporting Code. This would have been done long since but for the fact that earlier designs of Carrier-borne aircraft precluded the use of other than the simplest cryptographic aid in the form of Naval Aircraft Code and Syko (Nyko).

TOP SECRET

PART III - SECTION C-MERCHANT SHIPS' SYSTEMS.

Enemy successes in exploiting Merchant Ships' Code traffic have been reviewed in Part II, Section C. For the purposes of this section, these successes have been summarised into the following broad conclusions. In each case, the basic Merchant Ships' Code book is assumed to be compromised.

(a) General Systems. The established method of using a long-subtractor table as a General recoding system for communication with large numbers of Merchant Ships, all of whom hold the same series (the General and Indship Tables) is wholly unsound. A new system must be evolved.

(b) Convoy Systems. In order to achieve security for signals to all or individual ships in a Convoy, or stragglers from a Convoy, it was proved that a long-subtractor table, available concurrently to more than one originator, must be used in conjunction with a set of basic groups effective only for the passage of the Convoy concerned. (The "Diversion Code"). It was only by using such basic groups in recoding signals containing details of positions, routes, courses, rendezvous, destinations, etc., that we eventually succeeded in defeating the enemy Cryptanalyst.

(c) Communication with fast Independently routed Merchant Ships. There are sound reasons for believing that the "Oneship Pad" system proved secure, but there is no guarantee that it would have been so had the enemy devoted strenuous endeavours towards exploitation of traffic in these pads, since they were not "One Time". The system is, however, a sound one in principle, and should be retained in the improved form outlined below.

2. Future Policy-Recommendations.

(a) Basic Book. Book Code recoded by the subtractor

TOP SECRET

method should continue to be the standard system. The Basic Code should be a four-figure (instead of five-figure) one, and editions should be produced at a rate which will, in any future war, allow them to be changed every six months at least. Although, granted, we should at all times assume physical compromise of a book so widely held, and should design methods of recoding accordingly, this assumption is in itself no argument against neglecting the added precaution of frequently changing editions; moreover, even if an edition is not physically compromised, there is always to be reckoned with the danger that a proportion of basic groups will be recovered by the enemy in the course of his analysis of the vast quantity of traffic which must necessarily be coded in one and the same basic book.

(b) General Communications. For general communication with all Merchant Ships, there must continue to be available one General series of recoding tables. The stencil-subtractor system, with daily-changing Key Sheets, should, however, replace the long-subtractor tables.

(c) Communications with Independently routed Ships. In order to provide entirely secure communications from and to all independently routed ocean-going Merchant Ships, each of the latter should hold, (in addition to (b) above), a one-time subtractor pad (different for each ship) with 25,000 groups, made up of 100 pages, each with fifty lines of five groups. This new and larger style of "ONESHIP" pad would be used only for recoding signals of particular security importance such as those disclosing routes, positions, courses, rendezvous, etc. It is suggested that each pad should be divided into 20 Sections of five pages (1250 groups) each. The first two Sections of every pad to be marked exclusively for recoding signals originated

TOP SECRET

by the holding ship; the remaining eighteen Sections to be available for allocation, one each, to appropriate Naval Shore Authorities for recoding signals addressed to the holding ship. This type of true "One-Time" pad would replace the previous Oneship (but not one-time) pad. N.C.S.O's should hold stocks of pads for issue and replacement, as was the practice with Oneship pads. So far as replacement is concerned, it would be the duty of N.C.S.O's to scrutinise pads held by ships, and to issue a new one when there were indications that one or more Sections were nearing completion. Should a Shore Authority have completed his Section before a new pad was issued, he should notify the fact immediately to the appropriate Issuing Authority, with instructions to the latter to issue the ship concerned with a new pad at the next opportunity. Groups in a particular Section should never be used more than once. Pending, therefore, issue in these circumstances of a new pad, the originating authority concerned would communicate with the ship using the General (Stencil Subtractor) Table. Once issued with one of these pads, a ship should continue to carry it (or its replacement pad) regardless of whether she might subsequently sail in convoy.

(d) Convoy Communications. For communications from Naval Shore Authorities concerned with the routeing and direction of Convoys to one or all ships of an individual Convoy (including of course stragglers and joiners), it is recommended that the system of Diversion Codes with long subtractor table should be discontinued. Admittedly, the system proved generally satisfactory, but there are practical coding and security disadvantages attached to the use of one and the same set of subtractor groups concurrently by different originators and with two different sets of basic groups, i.e., those from the standard Merchant Ships Code and those from the special Diversion Code provided for each Convoy.

TOP SECRET

From every point of view, including the certainty of 100% security (which was not necessarily achieved by the Diversion Code system) it would be more satisfactory to make use only of groups from the standard Merchant Ships'Code, in conjunction,however,with a true one-time subtractor pad effective only for the passage of the one Convoy concerned. For this purpose it is recommended that "One Time Convoy Pads" should be produced. These pads would be similar to the proposed new style of ONESHIP (One Time) Pads described in clause (c), but very much smaller. It should suffice if a pad were to comprise 50 pages, each of 150 groups (30 lines of 5); i.e., a total of 7,500 groups. Each pad would be divided into ten Sections of five pages (750 Groups), and each Section should be reserved for exclusive use by one Naval Shore Authority. In common with the proposed new ONESHIP pad procedure, no recoding groups should ever be used more than once. In the unlikely event of a particular originator having exhausted his section before the Convoy had reached its destination, he should make use of the General Stencil Subtractor Table. In practice, however, it would doubtless be found that should such occasion arise he could, by arrangement, "borrow" unused groups from the Section allocated to another Authority. This would result in absolutely 100% secure communications to ships in Convoy.

3. There is no denying, of course, that the steps advocated above will involve production of S.Ps. on a very large scale. This should be undertaken in peace, and stocks distributed to focal points abroad to be held in readiness for issue in any future emergency. The resulting expenditure should be looked upon in the light of a ridiculously low premium towards a policy which will secure for us a really sound Merchant Ships' cryptographic system in any future "emergency". It would indeed be false policy, not to say utter folly, if we were to prejudice the safety of thousands of lives and vast tonnages of Merchant Shipping in the early stages of any future War, solely by allowing peacetime considerations of economy in book production to deter us from making advance arrangements in a form such as those advocated. In this connection, the disclosures made in Part II, Section C, and Part III Section E of this Review speak for themselves and provide an unanswerable argument in favour of such measures.

TOP SECRET

PART III - SECTION D - CALL SIGNS AND DELIVERY GROUPS.

A general survey of our War Call-Signs and Delivery Groups systems, together with a summary of enemy successes in breaking into them, has been included in Part II Section D. For the purposes of this Section, it will suffice to outline certain conclusions and recommendations in broad terms.

2. The Major War-Vessels system, which was effective for British use from the 1st February, 1944, onwards, proved itself to be secure and simple. It is recommended for retention as a Peace system, without use of the daily Index Numbers. It is well adapted for continued use in a future emergency, starting of course with new editions of Part I and II, and introduction of daily Index Numbers both for Call Signs and Delivery Groups.

3. The Minor War-Vessels system, i.e., the recoding of international signal letters, which was effective throughout the War and remains so, is, of course, very insecure, and the use of such call-signs also as Delivery Groups with codress messages contributed largely to the enemy's successes in breaking into traffic in Naval Code recoded by the Auxiliary Vessels' Recoding Tables. So long as a high-grade codress system remains effective for signalling with Auxiliary Vessels, there remains a danger to cypher security in using call signs such as these. Although admittedly no easy problem, it is obvious that serious consideration should be given to the evolution of a general system of call-signs and Delivery Groups applicable both to Major and Minor War Vessels.

4. So far as Merchant Ships' Call Signs are concerned, the system used during the War is a sound one and it is doubtful if any change is called for. Although it is true that such call signs were on occasions broken down by the enemy, this was due not so much to defects in the system itself, but rather to the fact that the enemy was able to decode much traffic in Merchant Ships' Code, and by this means succeeded in identifying certain call signs by equating them with the names of Merchant Ships appearing in decoded texts. The most serious danger to be reckoned with is undoubtedly the possibility of physical compromise

TOP SECRET

of a complete edition of S.P.02182, with the resulting compromise of the call signs of every Merchant Ship until such time as a new edition could be made effective. To counter this danger as far as possible, reserve editions of the Mercantile Secret Call Signs should be produced on a far more extensive scale than was the case during the War.

 TOP SECRET

PART III - SECTION E - GENERAL.

Enemy successes in reading individual types of high-grade and low-grade Naval codes and cyphers have already been described in the appropriate Sections of Part II of this Review. Further comments are, however, included in this final Section in order to provide a more co-ordinated picture of these achievements, and so help in forming a true appreciation of how the insecurity of our high-grade book systems, and Merchant Ships' codes, undoubtedly contributed to the appalling toll of Merchant Shipping losses during the Battle of the Atlantic.

2. From the outbreak of hostilities until June 1943, the Germans broke Atlantic area traffic in Naval Cypher and Naval Code with varying, but on the whole marked, success. They were particularly successful in exploiting traffic in the British-U.S. Naval Cypher, No.3, which was in force from before Pearl Harbour until 10th June, 1943.

3. They obtained from this source a great quantity of operational intelligence vital to them in their successful prosecution of the U-Boat war; e.g. convoy departure dates, routes, diversions, times and locations of change-over of Escorts, etc.

4. A comparable, although perhaps on the whole less serious, state of affairs resulted from the enemy reading traffic in Merchant Ships' codes. His successes were not, however, in this case brought to a conclusion in June 1943; they continued until the end of the war, except that, from 1st September 1944 onwards, he failed to break into the new and substantially improved Convoy system, i.e. the Diversion Code - Recoding Tables used for signalling routes, diversions, rendezvous, etc. to merchant ships in Convoy.

5. This deplorable record of enemy achievements is substantiated beyond doubt by (a) interrogation of high German Naval Officers and crypto. personnel, from Grossadmiral Karl Doenitz downwards, and (b) examination of the actual German Logs containing our decyphered signals.

TOP SECRET

6. So far as interrogations are concerned, there is a wealth of confirmatory material available, but it will suffice to quote here two extracts only:

Grossadmiral Doenitz: Doenitz stated emphatically that Signal Intelligence had been very valuable to him. It had been the best source of Naval Intelligence and, indeed, when air reconnaissance etc. was not available, had often been the only source of operational information.

In 1942, Signal Intelligence concerning convoy operations in the Atlantic had been of the highest order.

Obergefr. Holtermann, of the German Naval Crypto. Unit:

(edited extracts from a report written by this Officer in reply to a Questionnaire by TICOM).

With as little as 50 men, we could read the most important traffic until the beginning of 1943. The big Norway Attack was only possible because we could find out all the dispositions of the British Navy.

A big change in the set-up of the German Decoding Unit took place with the appointment of Grossadmiral Doenitz as C.-in-C. of the German Navy in place of Raeder. Doenitz took the Decoding Unit "under his protection", and from this moment it became one of the most important features in the Submarine Battle against England and U.S.A.

Nearly every U.Boat attack on a Convoy originated from the receipt of information regarding the Convoy's departure date, obtained from decoding signals. Submarines deployed over "hundreds of miles" could be ordered to concentrate for attack in a given position. This was achieved mainly through reading Naval Code.

Until July 1943, we had good results with the British-U.S. Naval Cypher (No.3), and could read nearly 30% of all intercepted traffic in this system. We could not read it all, because we had not time to decode every signal. Only the most important traffic was tackled; mostly Halifax and Freetown Broadcasts.

TOP SECRET

7. So far as examination of German Signal Logs and Signal Intelligence documents is concerned, it is unnecessary to quote more than one disastrous episode: namely, the U.Boat attacks on Convoys HX.229 and SC.122, in March 1943.

U.Boats first made contact with HX.229 on the evening of 15th March, 1943, and attacks on that Convoy, and on Convoy SC.122 in the same area, were carried out from 16th to 19th March inclusive, resulting in the sinking of 22 ships.

There is indisputable evidence from the German Signal Logs that the U.Boat successes on this occasion were mainly achieved owing to the breaking of our cypher traffic. Up till 16th March, i.e. the date on which the first attacks were made, the Germans had succeeded in reading no less than 16 signals concerning the movements of both Convoys. These included two very important ones made in the fatally insecure British-U.S.Naval Cypher No.3; viz: Commander Eastern Sea Frontier's 2210 of 4th March, giving ocean routes and stragglers routes for Convoy HX.229, and a signal from Halifax, 1932 of 13th March, containing diversion orders to both Convoys.

8. Enemy successes in breaking into our codes and cyphers are attributable almost exclusively to his cryptanalytic skill. An insignificant proportion only of his successes was the result of capture by him of code and cypher documents. In the latter connection, an Appendix is attached showing what appear to have been the main "pinches" throughout the war.

9. There is ample evidence to show that the enemy crypto.organisation was throughout the war handicapped by Staff shortages arising out of the man-power situation in Germany, and that if adequate personnel had been made available by the High Command for training as cryptanalysts, there would have been a substantial increase in the sum total of Signal Intelligence available to the enemy. In practice, the German Naval Unit had to discard a great proportion of intercepted material which, given sufficient staff, they could have worked on with good prospects of success, in favour of concentrating most of their attention upon traffic in the vital Atlantic area.

10. The German Crypto. Organisation maintained liaison with their Italian

TOP SECRET

and Japanese equivalents, and also with Finland in so far as Russian Cyphers were concerned. Although this liaison involved a considerable interchange of information, it is clear that the Germans were throughout very loath to disclose to their Allies full technical details of their work, and that they rated the capabilities of Italian and Japanese cryptographers as very low in relation to their own. The Germans do not appear to have co-operated in this respect with Hungary or Rumania. They established an organisation in Spain, however, and maintained a D/F Station there under German Naval control.

11. The Germans say they had no organisation for studying the Press for publication of unparaphrased versions of coded messages. They obtained little assistance from re-encypherments or from faulty verification, check and repetition procedure. So far as re-encypherments are concerned, they did, apparently, give the matter some attention, but without appreciable results.

12. Despite the success achieved by the Germans, up till June 1943, in exploiting our high-grade book systems (notably the British-U.S. Naval Cypher No.3), no plans or details concerning the one major Allied Amphibious Operation launched in that period (Operation "Torch") appear to have become known to him from cryptanalysis. This can no doubt be accounted for by the fact that in planning this operation (and all later major combined operations) One-Time systems were used almost exclusively, or, when a One-Time system was not available, signals were encyphered in machine systems using special Drums and/or Keys having a very restricted use.

This, however, is but small consolation in the face of the German achievements in breaking so much of our vital Battle of the Atlantic signal traffic.

13. In the final event, the "Lesson Learnt" is clear: namely, that the twin sciences of Cypher-making and Cypher-breaking are in their technique so closely related as to be indivisible; neglect therefore, in Peace, consistently to develop, improve and systematically attack our own cryptographic systems in relation to our contemporary knowledge and skill in Cryptanalysis, will assuredly mean disaster for us in a future war.

TOP SECRET

14. In concluding this Review, it is fit again to sound a warning note on the score of increased financial expenditure which will be involved in the process of developing our cryptographic systems along the sounder lines advocated. This point has already been mentioned on page 116, when discussing future Policy for Merchant Ships' communications. Let it however be repeated here that, whilst accepting the need for stringent National Economy during the lean years which lie ahead, we should have cause bitterly to repent if the Economy Drive were pressed to a degree which would preclude expenditure necessary to the technical and scientific development, and production, of really sound codes and cyphers. We have indeed been warned, and we shall at our national peril disregard that warning.

Naval Staff,
Signal Division and Intelligence Division,
Admiralty,
November 1945.

W.G.S.Tighe.
COMMANDER (S), R.N.

TOP SECRET

APPENDIX to PART III - SECTION E.

Enemy "Pinches"

(a) Bergen, May 1940

A copy of Administrative Code, which had been in force since 1934 and was replaced by Naval Code on 20th August 1940. Its capture can have been of little practical value to the enemy, since he had largely reconstructed the Code during its prolonged period of use.

A copy of Inderdepartmental Cypher No.1, in force since before the war and up till 15th June 1943. Little used for Naval traffic after introduction of Naval Shore Code in the middle of 1941.

Several copies of Merchant Navy Code and recoding tables. The Code was in force from 11th January 1940 until 15th April 1942 and was always assumed to be compromised.

One edition of Call Signs and Delivery Groups and instructions for their use. The precise edition is not known, but is one which the Germans stated was brought into force later.

A copy of Auxiliary Code and Recoding Tables. The Code was in force from before the war until 20th August 1940 when it was replaced by Naval Code. The Recoding Table captured appears to have been a current one, but it was replaced on 23rd May 1940.

(b) Off Tunis, mid 1941

A number of obsolete recoding and recyphering tables recovered at a later date from H.M.S."Mohawk", torpedoed off Tunis on 16th April 1941.

(c) Crete, May 1941

A copy of Naval Code No.1, obtained from H.M.S."York" sunk in Suda Bay. The copy is stated to have been permeated with sulphuric acid, and it is not clear whether all or any portion of it could be recovered sufficiently to be of value. The Code was in force from 20th August 1940 until 1st January 1942.

(d) From a ship "in northern waters" about March 1942

A copy of Merchant Ships' Signal Book (Mersigs II). This code came into force on 15th April 1942 to replace the Merchant Navy Code (see (a) above) and remained in force for the remainder of the war. Always assumed to be compromised.

(e) Tobruk, end of 1942

A copy of Naval Code No.2. In force from 1st January 1942 until 1st March 1943.

(f) North Africa, November 1942

An edition of Fleet Code. This edition, No.27, was used only as an exercise edition and was in force for this purpose from November 1942 until August 1944.

(g) Various occasions

Issues of Admiralty Fleet Orders ("S" Series). Of these, the most useful to the enemy were the standard S.1, S.2 and S.10 Orders, dealing with W/T organisation and coding and cyphering instructions.

TOP SECRET

(g) Various occasions (contd)

A copy of S.10/1944 ("Notes on Coding and Cyphering") was also obtained by the Germans from H.M.C.S."Athabaskan", sunk in April 1944, and was of some value to him in confirming the accuracy of his work on the Stencil Subtractor recoding system.

Copies of Small Ships Codes, Syko and Nyko were also captured on different occasions, mainly from small craft. They cannot have been of appreciable value to the enemy, since he was normally able to exploit traffic in these systems by cryptanalysis.

Typex machines: One machine was captured by the Germans during the final stages of the French campaign in 1940, about the time of Dunkirk. Two, and possibly three, more machines were captured from the Army during the North African campaign. In all cases the machines were captured without drums.

Note: This List is a remarkably short one, and comprises only a a very small proportion of Signal Publications which, during the course of the war, we had necessarily to assume as compromised by falling into enemy hands. A point of particular interest is that apparently the Germans recovered no codes or cyphers from H.M.S."Hardy" after the attack on Narvik in April 1940. H.M.S."Hardy" carried a full Flotilla Leader's set of cyphers and codes, and the circumstances of her loss were such that all had to be assumed compromised. This resulted in serious disruption of the whole Navy's communication security arrangements over a considerable period, and gave rise to the decision to introduce Area recoding and recyphering tables and special tables for ships operating in dangerous waters (see pages 3 and 4 of Review).

TOP SECRET

INDEX

	Page.
Administrative Code:	
Use of	1
Replacement by Naval Code No.1	3
Enemy work on	69
Aircraft Reporting Code:	
Introduction of	52
Enemy work on	87
Anglo-French Codes and Cyphers:	
Use of	2, 3
Enemy work on	77
Anglo-Soviet Cypher	17, 20
Area Tables - provision and use of	4, 5
Authentication Tables	53
Auxiliary Code and Recoding Tables:	
Use of	1
Replacement by Naval Code No.1	3
Enemy work on	74, 75
Auxiliary Vessels Recoding Tables	
Use of	3
Left and Right Procedure with	6, 12
Heavy wear on	10, 12
Plaindress procedure with	12
"B" Groups (See Monitoring)	
British Cypher No.5 - use of	20
Call signs and Delivery Groups:	
Summary of systems used	97, 98
Introduction of 3-letter system, S.P.02396 series	12
Recoding of Delivery Groups	12, 13, 17
New system, using Key numbers	26
Enemy work on	98 - 100
Combined Assault Code:	
Production and use of	52
Enemy work on	82
Combined Cypher Machines:	
Production and use of	25, 36-38
Rotating Indicators	38
Revised Indicator procedure	38
Enemy work on	79
Commodores' Recoding Tables:	
Use of	54
Enemy work on	90
Conclusions and Recommendations:	
High-grade book systems	101-104
Ship Index	104
Indicator systems	104
Machine Cyphers	105-107
One Time Pads	106-107
Fleet Code	108-110
Small Ships' Codes	110-112
Syko, Nyko	112

TOP SECRET

INDEX (continued)

Page

Conclusions and Recommendations(contd):
Merchant Ships' Systems 113-116
Call signs and Delivery Groups. 117-118

Convoy Recoding Tables:
Introduction of(multiple alphabet)tables... ... 55
Subtractor Tables 58
Larger subtractor Tables.. ... ... 59, 60
Diversion Code Tables 60
Enemy work on 91-94

Convoy HX 229 and SC 122.. 121

Cysquare 51, 52

Dangerous Waters Recoding Tables:
Introduction of 3
Changes of series 4
Additional tables made effective.. 5

Delivery Groups (See Call Signs)

Doenitz - Evidence of Grossadmiral Doenitz 120

Excessive loads on long subtractor tables .... 20, 21,42-46 and chart.

Fleet Code:
Survey of use 48, 49
Enemy work on 80-82

General Recoding Tables for Merchant Ship Code:
Enemy work on ... ... 89-91,95,96.

Holtermann - Report by Obergefr Holtermann 120

Indicators:
Early systems 6
Introduction of disguised S.P.I.s 6, 7
Reversion to plain S.P.I.s 11
Table Indicator Books, S.P.2169 series... .... 11, 16, 23
Incorrect choice of Indicators 15
Reintroduction of disguised S.P.I.s.. 18
Effect of changes on enemy work 63-74

Indship Recoding Tables:
Introduction of 55
Change to subtractor tables 59
Automatic changes of editions.. 60
Enemy work on 91, 95-96

Interdepartmental Cypher:
Replacement by Naval Shore Code for certain traffic .. 9
Enemy work on 75-76

International Code- use as Merchant Ships system .. 54
Enemy work on 89, 96a

TOP SECRET

INDEX (continued)

	Page
Intercept Groups in GRAF SPEE and ALTMARK..	96a
Inter-Service Cypher:	
Introduction of	16
Enemy work on	76
Left and Right recoding procedure:	
Introduction of	5
Applicable to Auxiliary Vessels Tables and British-U.S. Tables	6
Effect on enemy work	63-74
Lettered Coordinates:	
Improved security	25
Enemy work on	88
Mercantile General Call signs..	58
Mercantile Secret Call signs-enemy work on..	100
Merchant Navy Code - introduction of... ...	54
Merchant Ships' Signal Book-introduction of	57
Merchant Ships' systems:	
General survey of systems used	54-61
Enemy work on	89-96
Monitoring parties in enemy ships	89, 96a
Naval Aircraft Code - use of plain groups..	88
Naval Code:	
No.1, introduction of	3
No. 2, "	14
No.3, "	21
No.5, "	28
Enemy work on Naval Code	69-74
Naval Cypher:	
No.1, use of	1
No.2, introduction of...	3
No.3, "	8
No.3, special review on	40 - 46
No.4, introduction of...	14
No.5, "	24
No.7, "	28
Enemy work on Naval Cypher...	63 - 68
Naval Shore Code:	
Introduction of, with Area Tables	9,10
General Recoding Table	18
Special Table for Reporting Officers..	28,29
Enemy work on Naval Shore Code	77
Oneship Pads:	
Introduction of	55
Method of use	58
Replacement arrangements	59
Enemy work on	94

TOP SECRET

INDEX (continued)

	Page
One Time Pads:	
Introduction of	55
~~Method of use~~.....	58-10, 13,14,67
Extended use of	9, 13, 14
Indicator procedures...	10, 19
Use of long subtractor tables as BTP	19
Use of OTPs without basic book ...	
Use of Admiralty Cypher Out Pads by U.S.Navy Department.	26
Issue of Western Approaches pads to U.S.warships	16
Effect of increased use on enemy work	66, 67
Recommendations for future policy..	106, 107,114-116
Operation OVERLORD - special arrangements.	27
"Pinches" by the enemy	124,125
Recoding and Recyphering Table:	
Revised system of distribution and use.	22, 28
Rates of change inadequate	14
Editions for major operations.. ...	18, 27
Re-encypherments:	
Neglect to take precautions	25
Little assistance to enemy	122
Reference Positions - coding in Merchant Ships' systems	57, 59
R/T Call Signs - new system	25
Secrecy classifications	17, 27
Ship Index:	
Introduction of	7
Assistance to enemy	104
Slidex R/T code - enemy work on	88
Small Ships Codes - survey of use..... ...	49-51
Enemy work on	83-86
Spelling:	
Excessive and unnecessary spelling.	26
Abolition of Single Letter Table...	7
Assistance to enemy...	103, 109
Stencil Subtractor System:	
Evolution of	15
Test by G.C.C.S.	23
Introduction of	24
Double conversion procedure	28
Enemy work on SS system	71-74
Use of, for Merchant Ships systems.	114
Strip Cypher - use of	38

TOP SECRET

INDEX (continued)

	Page
Syko:	
Survey of use	51, 52
Enemy work on	86-87
Proposed discontinued use	112
Typex:	
Survey of development and use	30-36
Enemy work on	78
Future policy	105